INTEGRATED NON-KINETIC OPERATIONS: THE FRONTIER OF WARFARE IN SEARCH OF DOCTRINE

BY

ERICKA R. FLANIGAN

A THESIS PRESENTED TO THE FACULTY OF

THE SCHOOL OF ADVANCED AIR AND SPACE STUDIES

FOR COMPLETION OF GRADUATION REQUIREMENTS

SCHOOL OF ADVANCED AIR AND SPACE STUDIES

AIR UNIVERSITY

MAXWELL AIR FORCE BASE, ALABAMA

JUNE 2010

APPROVAL

The undersigned certify that this thesis meets master's-level standards of research, argumentation, and expression.

_____

DR. EVERETT C. DOLMAN (Date)

_____

DR. HAROLD R. WINTON (Date)

DISCLAIMER

The conclusions and opinions expressed in this document are those of the author. They do not reflect the official position of the US Government, Department of Defense, the United States Air Force, or Air University.

ABOUT THE AUTHOR

Lieutenant Colonel Ericka Flanigan is an intelligence officer in the United States Air Force. She was commissioned as a Second Lieutenant in the United States Air Force in 1995 and earned a Bachelor of Science degree in Communications from South Dakota State University the same year. In 1999, while stationed at the National Air Intelligence Center, Pentagon, she earned a Master's of Arts in Broadcast Journalism from American University, Washington, D.C. At the Pentagon, she represented Air Force efforts for national-level policy and wrote National Intelligence Estimates with the Central Intelligence Agency. She became a briefer to the Chief of Staff of the Air Force during NATO operations against the Milosevic regime in 1999. In 2000, Lieutenant Colonel Flanigan supported a Joint Task Force effort in Bosnia where she led intelligence operations for sensitive peace-keeping NATO missions. In 2001, she served on General Norton Schwartz's personal staff at 11th Air Force, Elmendorf Air Force Base, Alaska. From 2002-2005, she commanded intelligence operations for all C-17 operations during the opening days of Operation Iraqi Freedom and ongoing efforts in Operation Enduring Freedom. From 2005-2008, she held various positions at United States Strategic Command, including heading the J2's Global Analysis Center, executive officer for the Director of Global Operations and served as the USSTRATCOM Commander's aide-de-camp.

ACKNOWLEDGEMENTS

I would like to acknowledge several people without whose support and help I would never have gotten off the ground with this study. My most sincere thanks go to Rear Admiral Doug L. McClain, Director of Global Operations, United States Strategic Command, and Brigadier General Michael J. Carey, Deputy Director, Global Operations, United State Strategic Command for granting me interviews and guiding me through the realities of the challenges surrounding the current non-kinetic fight. My genuine gratitude goes to them for their enthusiasm in sharing innovative ideas for improving the way we execute non-kinetic warfare.

I especially want to thank Lieutenant Colonel Nicholas Chavasse for the many valuable insights from the CENTCOM theater. His expertise provided most valuable insight through the lens which only comes from that of a warfighter in the current fight.

Additionally, sincere thanks go to Dr. Everett C. Dolman and Dr. Harold R. Winton for their patience in keeping me on track throughout this endeavor. Doctors Dolman and Winton have passion for education and have not only contributed greatly to the completion of this study, but whose selfless contributions continue to inspire so many future strategists.

Most importantly, I want to express my sincere appreciation to my family, for their love, patience and understanding during those times I was absent while conducting research for this study. Their presence was very important to me and made all the difference in ensuring my success in completing this work.

ABSTRACT

Cyberspace and space operations are fast becoming a highly valued strategic commodity. In a world of rapidly changing warfare, it is to the advantage of the United States to enhance the efficacy of non-kinetic operations. Updating non-kinetic doctrine through clarified authorities, improved processes, and increased operational expertise must be brought to the forefront of doctrinal attention. Findings within this research indicate several conclusive results. First, non-kinetic operations will continue to grow in scope and importance as both friendly and adversary warfare dependence on space and cybernetic operations increase. Second, as with any instrument of warfare, updated doctrine must accommodate non-kinetic operations to ensure efficient execution. Such doctrinal changes must reflect strategic and operational needs of United States warfare as they fluctuate with the adversary's use of cyberspace capabilities. Third, proper authorities for command and control purposes must be consistently and clearly communicated from the joint community across the combatant commands. In addressing these concerns, suggestions for authority issues with legal consequences for targeting adversary nets in the domestic realm will be offered and a recommendation for increased expertise in the area of non-kinetic operations will be proposed. Specifically the United States Air Force must establish an aggressive system to develop senior leaders with combined space and cyber operational experience to ensure strategic effectiveness of future non-kinetic warfare.

CONTENTS

FIGURES

Introduction

> *…there is in every battlefield a decisive point, the possession of which, more than any other, helps to secure victory, by enabling its holder to make a proper application of the principles of war…*
>
> -- Lieutenant General Antoine-Henri, Baron de Jomini (1838)

Today's operating environment allows combatants to operate on a low-technology budget with high-technology tools. Adversaries such as al-Qaeda and insurgent groups across the globe have harnessed a form of cyber capability that enables mature networks and facilitates coordinated acts of terror. These tools, though cheap and easy to obtain, have presented a new breed of networked insurgents that present coalition forces a dynamic set of new challenges. With these challenges come innovative ways of dealing with a serious strategic threat. Enter non-kinetic operations, specifically through space and cyberspace operations. When used in both an offensive and defensive capacity, these non-kinetic instruments add a much-needed weapon to the coalition's arsenal of warfare.

The aim of this study is to show that non-kinetic operations—specifically space and cyberspace operations—will continue to grow in significance as the character of war evolves. However, the sustained success of non-kinetic operations requires several evolutions of improvement in order to neutralize the adversary's technical tools. In order to capitalize on friendly capability, while negating adversary space and cyberspace operations, three main developments must advance: first, clarify non-kinetic processes and authorities; second, to update joint cyberspace doctrine; third, to develop non-kinetic operations experts who have wartime experience in both space and cyberspace operations.

Background

Non-kinetic operations are not new or revelatory; they have been evident for years. In the world of cyberspace, offensive hacking operations have been online since 1988, when the Massachusetts Institute of Technology's growing network was infected with the first Internet worm—placed there by a Cornell graduate student.[1] More than 20 years later, innovative cyber and space operations have found a home in ongoing operations in Afghanistan and Iraq. The use of non-kinetic operations in combat have proven effective and enabling; but growth and improvement must continually be pursued, for success lies in the balance if non-kinetic operations are allowed to stagnate in warfare.

The non-kinetic threat to American forces is growing both at home and abroad. To underscore the strategic threat, the Federal Bureau of Investigation claims that cyber attacks are the third greatest threat to national security, only behind nuclear war and weapons of mass destruction.[2] In recent years, several significant cases have become hallmark episodes in the growing domain of cyberwar. Some of the most renowned cases of cyberspace warfare have infected networks at the strategic level.

Probably the most infamous example of a strategic cyber attack occurred on 27 April 2007 when, in a matter of hours, websites of Estonia's government, newspapers, and leading banks had all failed. Estonian military command and control networks had been compromised. An adversary had invaded, assaulting hundreds of targets throughout the country; but there were no tanks rolling, no guns firing, no aircraft circling. This was a confrontation in which a computer

---

[1] Scott J. Shackelford, "Estonia Two-and-A-Half Years Later: A Progress Report on Combating Cyber Attacks" (4 November 2009) *Journal of Internet Law*, Available at SSRN: http://ssrn.com/abstract=1499849.

[2] Rick C. Hodgin, "FBI ranks cyber attacks third most dangerous behind nuclear war and WMDs," *TG Daily*, 7 January 2009, http://www.tgdaily.com/security-features/40861-fbi-ranks-cyber-attacks-third-most-dangerous-behind-nuclear-war-and-wmds.

network did the combat, launching attacks "from thousands of zombie private computers around the world."[3]

Estonia had been hit hard, and nearly the same scenario would play out one year later in Georgia. Just prior to the Russian Army invading Georgia, a massive cyber attack rendered ineffective the networked systems of the Georgian armed forces. Most seriously affected were the Georgian air defenses and countrywide command and control networks. As a prelude that helped shape the tactical and strategic environments, these non-kinetic operations had an enormous impact on the Georgian people, military, and government—before any bullets.[4]

The Estonian and Georgian examples demonstrate that non-kinetic operations are not just a whimsical Western weapon, but rather an effective tool of *strategic surprise*. Likewise, such non-kinetic operations can act as an asymmetric equalizer for conventionally less-capable enemies of the US. Conversely, the United States can use such capability to enhance combat effectiveness with strategic repercussions.

Defining the Terms

The definition of cyber warfare is open to interpretation, depending on capacity or purpose; and numerous definitions have been offered and debated.[5] For example, in his article "From Cyberspace to Cyberpower:

---

[3] Shackelford, "Estonia Two-and-A-Half Years Later," 1.

[4] Shackelford, "Estonia Two-and-A-Half Years Later," 1.

[5] Winn Schwartau defined *cyberspace* in 1994 as "That intangible place between computers where information momentarily exists on its route from one end of the global network to the other…the ethereal reality, an infinity of electrons speeding down copper or glass fibers…Cyberspace is borderless…think of cyberspace as being divided into groups of local or regional cyberspace—hundreds and millions of smaller cyberspaces all over the world." Winn Schwartau, *Information Warfare: Chaos on the Electronic Superhighway*, 2nd ed. (New York, N.Y.: Thunder's Mouth Press, 1996). Edward Waltz defined *cyberspace* in 1998 as the middle layer —the information infrastructure—of the three realms of the information warfare battle space. The other two being the physical and the perceptual. Edward Waltz, *Information Warfare: Principles and Operations* (Boston, M.A.: Artech House, 1998). In 2008, the National Security Presidential Directive 54, known as the "Comprehensive Cybersecurity Initiative," defined *cyberspace* as, "The interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries." *National Security*

Defining the Problem," Daniel T. Kuehl illustrated that definitions of cyberspace reflect the diverse character of its users and naturally vary with parochial descriptions of the term.[6] Kuehl compares over 20 definitions of cyberspace, leading one to the conclusion that tailored definitions of the same term are customized to fit the needs of particular organization or operational functions.[7] In this study, Department of Defense (DOD) definitions generally suffice. Cyberspace "is a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[8]

> "I believe there has been a decision by the US to close down these internet forums as part of their strategy of defeating al-Qaeda and to stop it getting attention in the Arab world." Dia Rashwan, Egyptian security analyst (*Daily Telegraph*, 22 Oct 2008).

Space operations in the context of this study primarily include those termed *Space control* and *Space force application* as defined in Joint Publication 3-14, Space Operations.[9] *Space control* includes offensive space control (OSC), defensive space control (DSC), and space situational awareness (SSA). OSC includes those operations intended to deny the adversary use of space. DSC protects one's own space capabilities, and SSA involves characterizing space capabilities in both the terrestrial environment and space domain.[10] *Space force application* comprises

---

Presidential Directive 54, Cyber Security and Monitoring (Washington D.C.: Government Printing Office,2008).

[6] Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in *Cyberpower and National Security*, ed. Franklin D. Kramer et al. (Washington, D.C.: National Defense University Press, 2009), 24-42.

[7] Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," 26.

[8] Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms*

[9] JP 3-14 Space Operations, 9 January 2009, xi.

[10] JP 3-14, II-7.

actual attacks against terrestrial-based targets accomplished through military weapons systems operating in or through space.[11] As cyber-doctrine evolves, parallel offensive (perhaps Offensive Counter Cyber), defensive (Defensive Counter Cyber), and situational awareness (Cyber Situational Awareness) distinctions will be useful.

Though space and cyberspace operations are distinguishable by definition, one should conceive of the two as being inseparable both in theory and practice. Cyberspace operations rely on space capabilities and physical assets that act as critical enablers of cyberspace potential. Likewise, cyberspace offers space operations a venue for wielding offensive and defensive space capability. Together, these technologies could be conceived of as co- or interdependent for operation and existence, which is why the concept of *integrated* non-kinetic operations is crucial to the following analysis.

Limitations

Although non-kinetic operations include strategic communications, propaganda, and information operations, these traditional disciplines are outside the scope of this research. For purposes of this study, non-kinetic operations will be narrowed to space and cyberspace operations. Given this narrowed focus, the aim of this inquiry is to investigate the efficacy of non-kinetic operations and to offer a rational discussion for what to date appears to be sub-optimally executed space and cyberspace operations. This study offers recommendations for improvements and methodologies that aspire to enhance efficacy of future non-kinetic warfare are offered in this study.

The study is further constrained by an information cut-off date of 1 April 2010. The fields of cyberwar and non-kinetic cyber and space operations are rapidly evolving, and this research represents analysis

[11] JP 3-14, II-10.

and projections based on information available from open or unclassified sources as of the date stated.

The Nature of Non-Kinetics

The invisible networks upon which cyberspace operates seem intangible, yet have very substantial effects on adversary operations if conducted effectively. Such was the case in September 2008 when al-Qaeda propaganda websites celebrating the September 11 attacks were hit by unknown cyber infiltrators.[12] Though non-attributable, suspicions were rife that the disruption was caused by indiscernible Western cyber operatives. "I think the Americans are behind this," said Egyptian security analyst Dia Rashwan. William McCants, who operates Jihadica.com website and who is a consultant for the United States Military Academy said, "I think it's probably being orchestrated by several governments. Whoever is doing this knows what they are doing. They are being surgically precise."[13] Carl von Clausewitz theorized that all war has its foundation in politics.[14] To the extent that is true, then all actions in war have political ramifications; and this may be the most potent result of non-kinetic space and cyberspace operations. Regardless of attribution, the cyber assaults on these al-Qaeda websites sent a clear message of political significance—your virtual presence on the Internet is known, and you are vulnerable.

Space and cyberspace operations have unique characteristics that distinguish them from land, sea or air; yet their influence potentially has just as much political strength as traditional hard power. Among these discernible characteristics are the indistinct boundaries that frame and govern space and cyber domains. In *The Political Mapping of Cyberspace,*

---

[12] "Al-Qaeda Websites Hit by Western Cyber Attacks," *Daily Telegraph*, 22 Oct 2008, http://www.telegraph.co.uk/news/worldnews/asia/afghanistan/3237930/Al-Qaeda-websites-hit-by-Western-cyber-attacks.html/, (accessed 15 March 2010).
[13] Ibid.
[14] Carl von Clausewitz, *On War*, edited and translated by Michael Howard and Peter Paret (Princeton, N.J.: Princeton University Press, 1984), 605.

Jeremy Crampton illustrates the power of cyber through theorizing its capacity for spatial policy-making.[15] Crampton argues that space and cyberspace operations can act as a geography in and of themselves. As such, Crampton explores the importance of conceptualizing cyberspace, politics, and ethics at a higher level of rationality. According to Crampton, cyberspace should not be sheltered in concept by physical space—as has been the case with the domain of space. Instead, people should expand their thinking about cyberspace issues and elevate it to a completely different level of contemplation when regarding use of cyberspace for military options. Considering these notions, non-kinetic operations may still seem ethereal to the traditional warfighter. To them, space and cyber capabilities are viewed as mere enablers for a more traditional style of physical warfare.

Conventional warfighters commonly perceive space and cyberspace's unique attributes solely for their ability to facilitate terrestrial warfighting methods. In a significant way, the traditional warfighter's perception of non-kinetic operations is correct. Possibly more than any other medium, space and cyberspace operations hold force-multiplier and force-enabling qualities. Evidence of this is seen in the growing dependence on systems such as the Global Positioning System (GPS) for navigation and military communications satellites (MILCOMSAT) for global command and control. The joint space and cyber planner must not only understand planning and operational considerations for employment of space and cyberspace capabilities, but also ensure their availability have knowledge of threats to those systems.

To properly conceptualize their values, space and cyberspace operations must be seen as inseparable functions both in theory and in practice. Each is dependent upon the other in terms of space assets and

[15] Jeremy W. Crampton, *The Political Mapping of Cyberspace* (Chicago, IL: The University of Chicago Press, 2003), 187.

cyber networking. For example, an offensive space operation requires command and control of a space-based asset via networked cyber connections from the command center to the operational space asset. Likewise, cyberspace operations are reliant upon space-based assets for relay of cyberspace communications in theater and global engagements. Without cyber support, no space *systems* today are operational; and without space integration (to include precise timing signals for network coordination), no current cyber *systems* are functional.

Thus, space and cyber planning must be jointly integrated into the crisis action planning process so these operations are fully considered in conjunction with kinetic options. But full integration has been rare in practice. For example, planners in USCENTCOM have tended to give non-kinetic space and cyber operations short shrift, perhaps because they have not been asking the right questions or establishing the right requirements for effective space and cyberspace operations. Major General Michael T. Flynn, CJ2 ISAF, stated of non-kinetic operations in theater, "I need someone worrying about this every day."[16] His concerns echo those of many senior leaders in the Department of Defense who have recognized the existing gap in attention to non-kinetic operations.

What Non-Kinetic Operations Bring to the Fight

Allies and adversaries alike have become networked societies with increasing dependency on cyberspace. America's ability to gain and maintain cyberspace superiority has become essential in the joint endeavor to deliver and conduct military operations worldwide.

Since the turn of the millennium, joint military operations have seen a revolution in military affairs allowed by cyberspace technologies. Advances have afforded the means to produce magnified effects on adversary systems that traditionally could only be attained via kinetic means of warfare. For example, cyberspace in Afghanistan is not only

[16] Brigadier General Michael Carey (Deputy Director, Global Operations, US Strategic Command, Offutt AFB, NE), interview by the author, 10 May 2010.

being used in offensive operations against the adversary, but is relied upon for force-multiplier capabilities that enhance friendly operations. According to Lieutenant General Keith Alexander, who is to be the head of the new US Cyber Command, coalition forces rely on cyberspace capabilities to coordinate intelligence, battlefield operations, and military integration from 40 countries in the coalition. In recent Senate confirmation hearings, Alexander said it is "not about an effort to militarize cyberspace," but rather to leverage technology in America's favor.[17] Cyber operations have the potential to sustain key military advantages over adversaries. But this potential will be realized only if vulnerabilities are mitigated and improved non-kinetic employment is sought.

Non-kinetic operations through space and cyber are significantly influencing traditional force projection from air, land, and sea. When coupled with information, such non-kinetic operations are what the Air Force's Deputy Chief of Staff for Intelligence, Surveillance, and Reconnaissance (ISR), Lieutenant General David Deptula calls the *information in war revolution.*[18] For example, in the past the Air Force had "a specific aircraft for collecting data, then a separate organization for analyzing it, and then another organization and system for distributing it."[19] This cumbersome process was time and resource intensive; but with the technology available today, this whole process can be done from one air platform at "near real time and at the speed of light—and from across the globe."[20] This study includes a refined

---

[17] Ewen MacAskill, "New Cyber Security Chief Warns of Internet Attacks," (guardian.co.uk: Guardian News & Media Limited, 21 April 2010). http://www.concept-team.ch/2010/04/21/new-cyber-security-chief-warns-of-internet-attacks/, (accessed 25 April 2010).
[18] David A. Fulghum, "Military Tech, Organizations Will Merge," *Aviation* Week, 13 April 2010.
http://www.aviationweek.com/aw/generic/story_channel.jsp?channel=defense&id=news/asd/2010/04/13/02.xml/, (accessed 25 April 2010).
[19] Quoted in Fulghum, "Military Tech, Organizations Will Merge," 1.
[20] Quoted in Fulghum, "Military Tech, Organizations Will Merge," 1.

framework for the use of space and cyberspace capabilities and their ability to affect efficiently targets in joint campaigns and operations.

Non-kinetic Operations in 2010

In today's fight, non-kinetic operations target insurgent assets that are technical in nature, such as a network of connected computers, an insurgent's laptop, or even cell phone encryption. Due to the nature of these targets, there are almost always secondary and tertiary effects for which non-kinetic planners must account. First, coalition planners must ensure that by taking out a particular target, they are not taking away a valuable source of intelligence. This was the case early in the war in Afghanistan when coalition forces targeted communications nodes that previously had been sources of intelligence collection for adversary communications.[21] With the kinetic elimination of these communication nodes, no further intelligence was collected; and in the end more harm was done by the intelligence gap that remained. To avoid such dysfunctional actions, like their kinetic counterparts, non-kinetic targets must continually be verified as viable for action with intelligence, surveillance, and reconnaissance operatives.

Second, non-kinetic planners must ensure appropriate levels of non-kinetic response. For instance, as in kinetic planning, consideration for appropriate damage, denial, or destruction is accomplished through dial-a-yield planning. Ironically, overkill through non-kinetic operations is possible and could produce a devastating mistake. Where technology allows, non-kinetic operations should be as surgical as possible. For example, if coalition forces in Afghanistan conduct an offensive cyber attack that takes down an entire community's power network, instead of just insurgent cells, then the operation was not likely planned or

[21] This is an example of how a post-strike scenario of an Afghani communications target could potentially eliminated intelligence collection benefits. Sayed Salahuddin, "Gunmen Destroy Mobile Phone Tower in Afghan South," Reuters, 2 March 2008, http://www.alertnet.org/thenews/newsdesk/ISL175699.htm/, (accessed 15 march 2010.)

executed with efficient precision. While finessing acute effects on the target, one goal of non-kinetic operations should be that of transparent or even non-attributable operations. Another methodology beneficial to non-kinetic operations is the ability to defer attribution in order to enhance denial and deception operations, or to augment ongoing psychological operations.

To the typical bystander, non-kinetic operations are not readily perceived. The effects are difficult to connect to specific non-kinetic operations. It is the user of that technology or targeted network who is directly affected. Non-kinetic operations typically do not leave a smoking hole, no audible violence, and no collateral civilian bloodshed. In this manner, non-kinetic operations are elusive. But they also represent a tremendously influential capability that should not be underestimated. They can also be discrete; precise; and, when desired, unattributable. To undervalue the power of non-kinetic warfare, and its resulting effects is to fail to understand integrated operations.

Chapter 1

Starfish and Spiders:
Understanding Networks for Non-Kinetic Effects

A brain is a society of very small, simple modules that cannot be said to be thinking, that are not smart in themselves. But when you have a network of them together, out of that arises a kind of smartness.

—Kevin Kelly

Hierarchy of Nets

The shape of today's adversary is not the convenient top-down hierarchical structure of the traditional nation-state opponent. Gone are the days where a predictable chain of command or strictly blocked pecking order lent itself to an easily targeted organization. The shape of today's adversary is one that requires creative planning, necessitates imaginative targeting, and demands ingenious techniques to influence it adversely.

In the traditional sense, a hierarchical flow would ideally affect insurgent operations as seen in Figure 1. However, the United States finds itself matched against an adversary that is not a centralized organization, but rather a decentralized set of networks loosely assimilated under common ideologies.

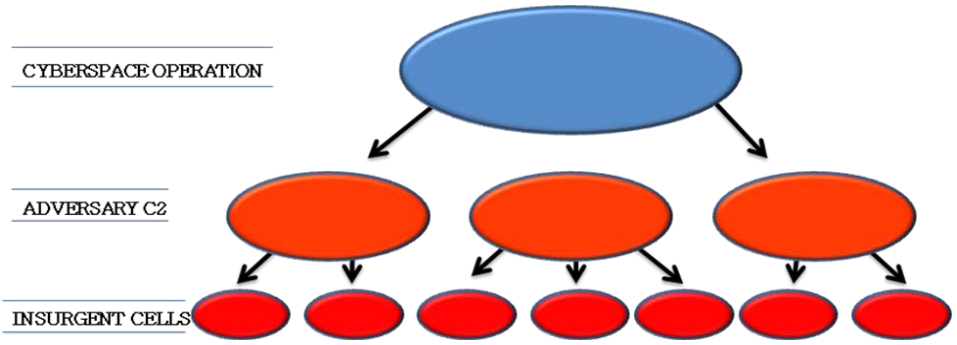

Figure 1: Non-Kinetic Operation Effects on Adversary Systems
(Source: Author's original work)

This concept parallels that described by John Arquilla and David Ronfeldt in their article, "The Advent of Netwar." According to Arquilla and Ronfeldt, the term netwar is defined as a "mode of conflict (and crime) at societal levels, short of traditional military warfare, in which the protagonists use network forms of organization and related doctrines, strategies and technologies attuned to the information age."[1] Arquilla and Ronfeldt continue by describing the leadership capabilities of such a network, in that "the organizational design is flat. Ideally there is no single, central leadership, command or headquarters – no precise heart or head that can be targeted."[2] This idea of an ostensibly leaderless organization is emphasized in Ori Brafman and Rod Beckman's work, *The Starfish and the Spider*. In it they relate two types of organizations: the spider type, analogous to a centralized hierarchy with a head, body, and legs, which dies if the head is removed; and the starfish type organization, analogous to a decentralized unit with no singular head or central organs, able to survive despite loss of limbs or other principal features of the system.[3]

> A coalition task force received intelligence that a coordinated attack was planned by multiple al-Qaeda cells throughout locations in Kabul. Coalition intel indicated the insurgent coordination for the attack would come via an encrypted satellite phone. Rather than hardening the intended targets, coalition non-kinetic operators infiltrated the insurgent comms and sent the would-be bombers into ambushes. (Information Operator in theater, December 2009).

When considering non-kinetic effects on centralized and decentralized target sets, planners must not neglect the power of

---

[1] John Arquilla and David Ronfeldt, ed., *Networks and Netwars* (Santa Monica, CA: RAND Corp., 2001), 6.
[2] Arquilla and Ronfeldt, *Networks and Netwars*, 9.
[3] Ori Brafman and Rod A. Beckman, *The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations* (New York: Penguin Group, 2006), 35.

intelligence regarding the contrasting organizations described by Brafman and Beckman. For example, the starfish theory of decentralization describes most insurgent groups as follows: "an open system doesn't have central intelligence; the intelligence is spread throughout the system. Information and knowledge naturally filter in at the edges, closer to where the action is."[4] Hence, in decentralized insurgent organizations, intelligence is spread around. It does not rest centrally with an agency that can distribute knowledge to its leaders and operatives. Each insurgent cell has limited leadership and intelligence associated with it; there is effectively no single point of failure toward which non-kinetic efforts can be leveraged. Finally, Brafman and Beckman insist that through history the starfish types of decentralized organizations habitually succeeded in challenging more traditional and centralized organizations. Historically, groups from aristocratic landowners in feudal Europe to defiant Native Americans in the western hemisphere exemplify this model. Today, groups such as al-Qaeda, international crime syndicates, and even cyber organizations such as Wikipedia all represent this type of starfish organization.[5]

The Anatomy of a Network

The decentralized nature of many insurgent cells is a key consideration for non-kinetic operations planners. A hallmark strategy for al-Qaeda continues to illustrate that decentralized command and control are critical to execution of coordinated attacks. By further understanding the anatomy of networks, a strategist can better determine how non-kinetic operations would ultimately work against them.

For the non-kinetic planner and operator, mapping and understanding the adversary's networks is vital to coalition space and cyberspace operations. Charting and recognizing adversary network

[4] Ori Brafman and Rod A. Beckman, *The Starfish and the Spider,* 40.
[5] Unpublished paper. An Information Operations Officer, Task Force Iron. "Deception 2.0: Deceiving in the Netwar Age."

structures through social network analysis (SNA) methods allow planning and execution of non-kinetic operations against them.[6] Current US Joint Counterinsurgency doctrine characterizes SNA as "a tool for understanding the organizational dynamics of an insurgency and how best to attack or exploit it. It allows analysts to identify and portray the details of a network structure."[7] SNA shows how an insurgency's network organization acts and how a networked relationship affects its behavior, especially in its ability to operate, train, and equip.

According to US Army Field Manual 3-24, the US Department of Defense (DOD) uses SNA to analyze the design of a network for many reasons, all of which help in understanding the adversary. One primary use is to determine if components of that network are able to operate independently.[8] Additionally, analysis of the social network may indicate the location of an adversary's leadership or how hierarchical the organization is. After DOD analysts establish a good foundation based on study of an adversary's social network, further dynamics of the adversary's organization might be realized. Among the most valuable-added benefit of SNA is insight on an organization's ability to adapt when its environment changes or when coalition forces influence a change to its social network.

Military analysis of an adversary's SNA is built on relationships of actors, or nodes, whose links indicate connectivity to associated actors. A pictorial representation of nodes indicates the dynamics of related actors and allows monitoring of network growth, density, and, ultimately, its capability to operate. For instance, an increase in network activity

---

[6] Excellent overviews of SNA are available in Linton Freeman, *The Development of Social Network Analysis: A Study in the Sociology of Science* (Vancouver: Empirical Press, 2004); John Scott, *Social Network Analysis: A Handbook.* 2nd Ed. (Newberry Park, CA: Sage, 2000); and Duncan Watts, *Six Degrees: The Science of a Connected Age.* (New York: W. W. Norton & Company, 2004).
[7] US Army FM 3-24, *Counterinsurgency Field Manual*, (Chicago, IL: University of Chicago Press, 2007), 317.
[8] US FM 3-24, 317.

between nodes indicates the likelihood that a group has the ability conduct coordinated attacks.[9]

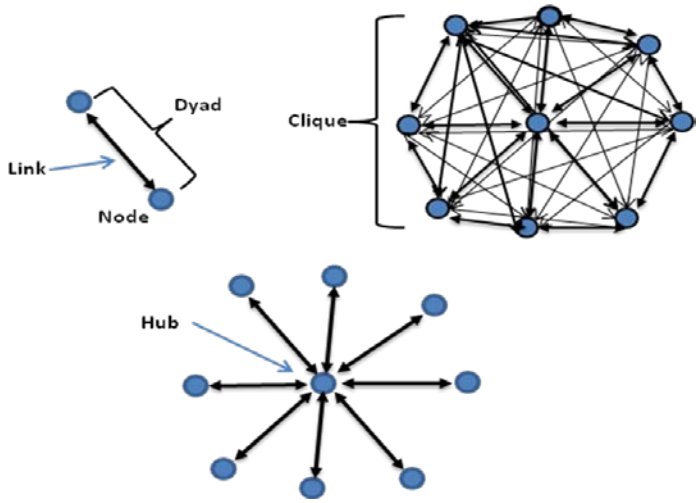

Figure 2: Network Components (arrows represent the direction of information flow)
(Source: Author's original work)

As dependable as it may appear, the efficacy of SNA is debatable based on several variables that may negate its reliability. First, this analysis takes time to develop, after which it requires constant monitoring to distinguish between routine and anomalous activity. Second, studying network density may not provide effective indicators depending upon the organizational type. For instance, a more centralized network "dominated by one or a few very connected nodes" may not accurately identify those decentralized actors who have few connections to the representative whole.[10] Yet in an insurgency, these decentralized nodes may be the operators who actually carry out acts of terror. Third, if SNA produces a biased network assessment, a flawed evaluation of the entire organization could result. The preceding arguments are recognized limiting factors of SNA; however, for the purposes of non-kinetic operations, SNA should be considered a viable

[9] FM 3-24, 320.
[10] FM 3-24, 320.

form of adversary analysis as long as thorough SNA corresponds with other adversary indicators and intelligence sources.

Military SNA is highly developed, and complex. For the argument that follows, an understanding of characters and their relationships to one another illuminates the efficacy of SNA and how non-kinetic operations might influence a network's components. These should comprise all relevant actors of a network, to include the leadership, facilitators, and operators. To underscore the importance of network analysis, the focus now shifts to a brief discussion of degree centrality and its role in network-oriented non-kinetic operations.

Experiences in Iraq show that the mavens— *inspirational figures of an insurgent group—tend to be logistical and financial actors in the network, and are often more valuable non-kinetic targets than the leadership.*

Brafman and Beckman refer to the key nodes in a network as *catalysts*. These often take the form of an "inspirational figure who spurs others to action."[11] Malcolm Gladwell calls these types of people *mavens,* who "are really information brokers, sharing and trading what they know."[12] For targeting purposes, knowing the network and the power of the mavens is key to effective non-kinetic operations against such a target. Arquilla and Ronfeldt make a similar point when they write "power and influence depend less on one's personal attributes than on one's interpersonal relations—the location and character of one's ties in and to the network."[13] These nodes have high credibility with those nodes to which they are linked; therefore, information flowing through them will most likely be considered convincing—and most acted upon.

Augmenting the centrality argument is a node's level of degree centrality: the number of node connections and the ease with which a

[11] Brafman and Beckman, *The Starfish and the Spider*, 93.
[12] Malcolm Gladwell, *The Tipping Point* (New York: Little, Brown and Co., 2002), 69.
[13] Arquilla and Ronfeldt, *Networks and Netwars,* 317.

node connects to other nodes. Gladwell refers to these types of nodes as *connectors,* or "people whom all of us can reach in only a few steps because, for one reason or another they manage to occupy many different worlds and subcultures and niches."[14] In essence, this is the same concept as "six degrees of separation": who is connected to whom in the shortest distance possible.[15] One may initially conclude that the leader of an insurgent group is by definition a primary *connector* node. While this can be the case, in reality it often is not. For example, a courier or a weapons distributor may have much more immediate connections to members of the insurgent group than does its leader. By ensuring information gets to a *connector* there is a high probability the message will reach many other nodes and cliques in the network. Appreciation of such nodal analysis is critical for non-kinetic operations, where the most valuable target very well may not be the leader.

The key to planning and executing non-kinetic operations against a networked adversary lies in targeting the mavens and connectors, not in targeting leadership. Caution is required, however. There is a general tendency to target (and effectively purge) those nodes that have a high degree of centrality, but often this can have negative consequences. Brafman and Beckman assert, "If a catalyst is killed, the power shifts to the circles, making the organization that much more decentralized."[16] As such, cells will become even more independent and continue to function—albeit with less interaction across the network.

---

[14] Gladwell, *Tipping* Point, 48.

[15] The Six Degrees of Separation concept (or the "Human Web") was popularized by John Guare. The concept offers the notion that if a person is one step away from each person they know, then everyone is at most six steps away from any other person on Earth. John Guare, *Six Degrees of Separation,* stage play *(New York, N.Y.: Dramatists Play Service, Inc., 1990)* premiered Mitzi E. Newhouse Theater, New York City, NY, 16 May 1990. See also Duncan J. Watts, *Six Degrees: The Science of a Connected Age* (New York, NY: W.W. Norton, 2003).

[16] Brafman and Beckman, *The Starfish and the Spider*, 143.

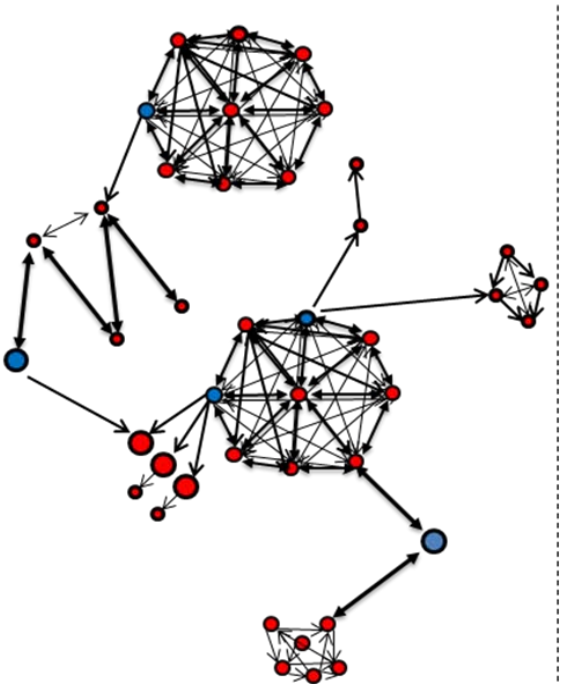

Figure 3: Insurgent Network with mavens in blue
(Source: Author's original work)

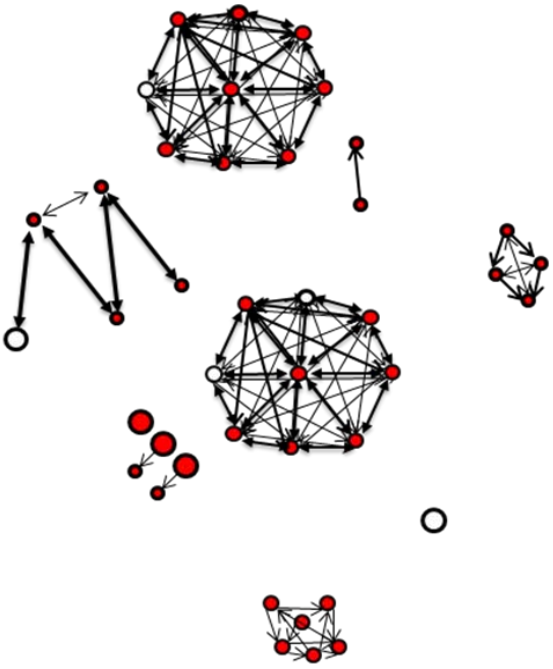

Figure 4: Fractured Insurgent Network, post - targeting of mavens
(Source: Author's original work)

Space and cyberspace operations bring considerable capabilities to nodal analysis. For example, cyberspace operations can insert one's own information into the targeted network at critical points where the messages and observables will resonate with the greatest impact. However, in a leadership node, the goal is to get information *to* those critical mavens or catalysts that will have the highest degree of net influence. By having the maven or connector node spread deceptive information throughout the insurgent cell, or accurate information that could work against the cell, the information will carry with it a significant amount of credibility, often more so than if the cell comes across the information on its own.

The logic here is consistent with emerging trends in the so-called Information Age, presaged by the eighteenth-century Smithian free-market attack on mercantilism. It is not the individual or state that hoards the most information (or gold, in Adam Smith's assessment) that has real power, but the one that provides the most *useful* information (or

gold in the form of capital investments) that prospers. The operating environment for non-kinetic cyber operations today is one of information abundance—not scarcity.

A Brief Case Study – Task Force Iron, Non-Kinetic Lessons in Iraq

The practice of pursuing mavens or catalysts with non-kinetic operations occurred during Operation Iraqi Freedom (OIF), albeit mostly through trial and error. Initially, coalition planners followed doctrinal methods beneficial to coalition objectives. The non-kinetic focus was on insurgent leaders. A problem arose when it was discovered that too many insurgent leaders were based on geography or ideology; leaders appeared to be everywhere. In his article, "A Social Network Approach to Understanding an Insurgency," Brian Reed points out that a group "like al-Qaeda cannot, in theory, be deterred because it has no easily identifiable hierarchy or location."[17] Planners had to find a different targeting construct for non-kinetic operations. Social network analysis revealed a new approach. Using software programs such as Analytic Technologies' UCINET software package and applying existing *Analyst Notebook* charts, social network analysis was conducted by Task Force Iron's Information Warfare Cell.[18] Task Force Iron then focused on nodes identified as having the greatest network centrality, which, it soon became apparent, were not the insurgent's leadership. In one particular circumstance, a non-kinetic operation targeted a connector who was linked to over 100 other suspected insurgents. In the months that followed, reactions from non-kinetic targeting of the mavens and connectors began to show results, as multiple reports indicated

---

[17] Brian Reed, "A Social Network Approach to Understanding an Insurgency," *Parameters*, Summer 2007, 27.

[18] Unpublished paper. The Information Warfare Cell for Task Force Iron was the name given to the cell in the deployed theater of operations. This cell dealt with Information Operations against specific targets in the USCENTCOM AOR. SNA software tools are abundant. For an overview of the most common, see Mark Huisman and Maritje Van Duijn, "Software for Social Network Analysis," in Peter Carrington, John Scott, and Stanley Wasserman (Eds.), *Models and Methods in Social Network Analysis* (New York: Cambridge University Press, 2005), pp. 270–316.

successful influence throughout the insurgent networks.[19] By the end of Task Force Iron's tour in Iraq, this form of non-kinetic targeting had become a standard operating procedure.

Changing the paradigm for non-kinetic targeting to one based on the Netwar concept was not the only one Task Force Iron learned during missions in northern Iraq. Other lessons held equivalent significance. [20] One of the biggest fears when executing non-kinetic operations through cyberspace for misinformation purposes is that the misinformation will destroy allied force credibility within the local populace. One commander in theater went so far as to say that in a counterinsurgency, "you should never try to implement any sort of IO *deception* operations."[21] The rejoinder to this dilemma, however, resides in preparing observables that mitigate this risk.

Task Force Iron's most successful efforts occurred when it used counterintelligence channels to deliver disinformation to the insurgent networks. This approach has historic validation. In Thaddeus Holt's *The Deceivers*, a study of World War II espionage, "double agents had had far more influence than the elaborate efforts at signal deception."[22] Likewise, during the 2006 conflict between Israel and Hezbollah, the turning of several Israeli agents in southern Lebanon provided Hezbollah the ability to conduct significant operations against Israel.[23]

Dispelling Myths of Non-kinetic Warfare

An often misunderstood concept associated with non-kinetic operations is that they are resource intensive. Task Force Iron found

---

[19] Interview with Information Operator in theater, December 2009.
[20] Arquilla and Ronfeldt, *Networks and Netwars,* 317.
[21] Ralph O. Baker, "The Decisive Weapon: A Brigade Combat Team Commander's Perspective on Information Operations," *Military Review,* May-June 20067, 21.
[22] Thaddeus Holt, *The Deceivers* (New York, NY: Scribner, 2004), 779.
[23] Alistair Crooke and Mark Perry, "How Hezbollah Defeated Israel: Part 1: Winning the Intelligence War," *Online Asia Times*, 13 October 2006, http://www.atimes.com/atimes/Middle_East/HJ12Ak01.html/, (accessed 18 February 2010).

this was not accurate.[24] Gone are the days of conducting massive feints or using friendly force maneuvers to deceive an adversary. Such tactics are virtually irrelevant for the network conflicts coalition forces find themselves in today. For example, due to widely available information technologies and networking, insurgents know when allied forces leave the perimeters of their camps. Any physical movement is difficult in a world of camera-phones, proliferated social-networking sites, and 24-hour news reporting. The attractive nature of utilizing non-kinetic space and cyberspace operations is that coalition operators can influence insurgents with little or no delay and no physically observable tip-off indicators.

Accompanying cyber and space operations in this regard are simple, low-technology deceptive operations. For example, in Iraq coalition forces have experienced more success through a notebook falling from a helicopter than by moving a company of infantry across a province.[25] Mentioning a piece of information in an engagement to a local businessman suspected of being linked to several terrorist groups carries with it more weight than a demonstration by friendly troops. Holt implicitly stresses the comparison in World War II: "the resources devoted to deception … were trivial in terms of the Allied war effort."[26] Similarly, resources devoted to non-kinetic operations in Afghanistan and Iraq should maintain a relative low visibility and leave a small footprint but have a powerful influence on adversary capability.

For Task Force Iron in Iraq, the goal of influencing insurgents either to act or not act through non-kinetic operations did not change. What did vary was how non-kinetic targeting was pursued. Targeting of the insurgents' command and control was no longer a focus. Rather non-kinetic operations focused on the nodes within the network that had the greatest potential to communicate with a majority of the networked

[24] Interview with Information Operator in CENTCOM theater, December 2009.
[25] Interview with Information Operator in CENTCOM theater, December 2009.
[26] Holt, *The Deceivers,* 781.

cliques or cells. Aiming for such targets allowed non-kinetic operations to be passed across the network to various cells and greatly aided in achieving the desired effects. Thus, many of the adages of old are applicable to today's fight. Non-kinetic operations will continue to be a critical tool in wars to come, and will be even more effective if brought to bear against those adversarial elements most connected to the others.

In summary, today's adversary is linked via a network of actors. Like severing the legs of a starfish or spider, adversarial networks are vulnerable to being crippled by cyber or space operations. For coalition forces conducting such non-kinetic targeting, operations have proven less resource intensive than initial popular perception predicted. Additionally non-kinetic options allow coalition forces to have the benefit of relative transparent action while effecting an enemy target set with influential resolve.

Chapter 2

Non-Kinetic Warfare: Today's Enabler, Tomorrow's Operator

> *We have moved past the civilities in the cyberspace domain. United States forces and those of our adversaries now rely heavily on their computer networks for command and control, intelligence, planning, communications,* and conducting operations.
>
> -- *General Kevin Chilton*

A Glance Forward

Imagine for a moment warfare in the year 2030. What will traditional kinetic warfare look like? Picture a battle-space where all weapon systems automatically transmit critical data, machine-to-machine, through a network of cyber and space-based relays, protected by multilayer security, to the appropriate command centers where planners, analysts, and commanders see a concurrent representation of the status of those assets. The commanders receive the information, not in raw format, but with fused intelligence via machine-processing to create conclusive options for decision makers. In this future scenario, space and cyber have more than *enabled* the future warfighter. Space and cyberspace operations have *become* warfighters in their own right. That is where we are going.

What then do space and cyberspace operations offer national security planners in 2011? Emily O. Goldman captures the answer to this question in one broad yet thought provoking concept. According to Goldman, national security rests on the retention of informational superiority, which can be competed for and won through space and cyberspace operations.[1] Goldman states, "the response to information age multidimensional conflict cannot be a response to an event (11 September), but must be an answer to an inexorable emergence of a new

[1] Emily O. Goldman, *National Security in the Information Age* (Portland, O.R.: Frank Cass Publishers, 2004), 42.

dimension of security competition."[2] As demonstrated in the Cold War, nothing drives weaponry advance like security competition. In this case, space and cyberspace are simultaneously emerging as the next generation precision weapon, ready at moment's notice and as responsive as the speed of light.

To Compel or Deter: That Is the Question

Non-kinetic operations might be thought of in terms of Thomas Schelling's bargaining power concept, where military force is weighed relative to its ability to deter or compel. In Schelling's writings, deterrence and compellence are carefully defined. Deterrence means "to prevent from action by fear of consequences"; compellence means "to make others act."[3] As such, Schelling stated that deterrence tends to be indefinite in its timing, while compellence has to be specified. In this formulation, non-kinetic operations through space and cyberspace are more analogous to compellence than deterrence.

A Coercive Operation: A coalition Task Force sent a bogus command through insurgent texting channels informing a small cell to swap their current phones for new ones. A date and place for the exchange was arranged with a trusted informant where 90 percent of the insurgents were successfully compelled to hand over their phones. Each received a new phone, and none was the wiser.

Robert Pape's account of coercion offers a useful framework for non-kinetic operations. Pape argues that "coercion seeks to achieve the same goals as war fighting, but at less cost to both sides."[4] In this sense, the coercive capability of non-kinetic operations holds the benefit of addressing an adversarial target without necessarily invoking visible violence upon

[2] Goldman, *National Security*, 42.
[3] Thomas C. Schelling, *Arms and Influence*, (New Haven, CT: Yale University Press, 1966), 71.
[4] Robert Anthony Pape, *Bombing to Win: Air Power and Coercion in War*, (Ithaca, NY: Cornell University Press, 1996), 13.

that adversary. Certainly the benefits of non-kinetic coercion are strong whenever non-kinetic operations can have effective compellence or coercion power while not harming civilians or causing collateral damage.

Non-Kinetic Warfare via the Adversary's Backyard

For strategists, compellence, deterrence, and coercion are relevant concepts to ponder when considering cyberspace operations grounded in both defensive and offensive capabilities. As in mathematics, non-kinetic warfare has constants and variables. In the case at hand, today's constant is the insurgent. The always-changing variable is the way the insurgent uses cyber resources. For this reason, it has been critical for coalition non-kinetic planners and operators to recognize changes to insurgent cyber practices and to tailor friendly operations to reflect those adaptations. Moreover, coalition forces must be cognizant of the passive observer, the cyber warriors from third-party nations whose monitoring of coalition non-kinetic actions may in turn be helping them learn how Western forces operate. The challenge for coalition non-kinetic operations, especially in the USCENTCOM area of responsibility, involves the very region in which it operates.

The renowned real estate mantra *location, location, location* applies to the non-kinetic warfare environment. For example, in Afghanistan the networks are owned and operated by America's potential strategic competitors: China, Russia, and Iran. In Iraq, the non-kinetic neighborhood has a bit better curb appeal. It is more operationally pleasing, more safe to walk the streets. However, Iraqi nets are also being monitored by strategic adversaries. With these important factors at the forefront of planning, appropriate use of non-kinetic operations may be achieved. Nonetheless, given the sketchiness of the neighborhood, one should constantly be aware of one's surroundings. For example, if non-kinetic operations aim to neutralize a network in Mosul, Iraq or in Herat, Afghanistan, coalition forces may be tipping their hand to others (such as Russia, China, or Iran) on the net who just

happen to be in the area casually observing. If this happens, coalition forces may not even be aware of the strategic gain awarded the opponent. Another consideration is the nuclear club—Pakistan, India, China, Russia, and probably soon-to-be Iran, who are all in the neighborhood in which cyber operations are being conducted. Now we have moved beyond a tactical level of an outwardly simple non-kinetic operation. The implications of non-kinetic warfare in this case have become strategic concerns; and when nuclear states are in play, the stakes of war are higher. This considerations raise the question, what will other nations deem an *act of war*?[5] Where will most countries draw the line and start considering non-kinetic operations *acts of war*?

A Persistent COIN Environment

Military use of non-kinetic operations has keen value in Iraq and Afghanistan for a variety reasons. For instance, adversaries in both Iraq and Afghanistan have turned to network technologies to continue their insurgent ambitions. Therefore, today's coalition warfighter has a set of unique challenges that blend traditional COIN with the latest innovative and technology-savvy terrorists. In this environment, high-technology tools augment the cultural and social behavior characteristics of insurgents. Anthropologist Montgomery McFate argues that a newfound imperative for cultural knowledge about the insurgents is vital to non-kinetic operations in a COIN environment.[6]

"Traditional methods of warfare have proven inadequate in Iraq and Afghanistan," says McFate. Thereby the role non-kinetic operations plays in COIN operations is decidedly validated.

[5] An *act of war* is typically defined as "an aggressive act that constitutes a serious challenge or threat to national security, armed conflict, whether or not war has been declared, between two or more nations; or armed conflict between military forces of any origin." Kevin Coleman, "What Constitutes an Act of Cyber War?" *Defense Tech,* 18 June 2008, http://defensetech.org/2008/06/18/what-constitutes-an-act-of-cyber-war/, (accessed 18 March 2010).

[6] Montgomery McFate, "Does Culture Matter? The Military Utility of Cultural Knowledge," *Joint Forces Quarterly* 38 (Summer 2005), 46.

Non-kinetic options in a COIN effort *should* seek to influence insurgent strategy. However, experience in the last decade has demonstrated surprising insurgent resilience. Undeniably, the insurgents have done far better than anticipated. In 2008, al-Qaeda celebrated a momentous occasion with the twentieth anniversary of its founding. Well-known terrorism scholar David Rapoport estimated in 1992 that the life expectancy of a Cold-War era terrorist organization was less than a year.[7] Now, fast-forwarding to the twenty-first century, contemporary research by Audrey Kurth Cronin shows the average life span of a terrorist organization is between five and ten years.[8] Statistically, modern terrorist groups are demonstrating endurance much greater than those of the past. Specifically, al-Qaeda has shown an uncanny ability to persevere and perhaps even *thrive* as an insurgent assembly in a world in which major powers still extort great influence. This unexpected endurance is one in which kinetic operations have proven only marginally effective. This situation calls for alternative employment options for non-kinetic warfare in the areas of space and cyberspace.

Al-Qaeda's resiliency is indeed remarkable. First, al-Qaeda not only survived the post-9/11 onslaught of American superpower in Afghanistan, it maintained its worldwide nodes. Second, al-Qaeda has achieved household name recognition around the world. If celebrity was ever its aim, al-Qaeda has achieved nothing short of global notoriety. Third, al-Qaeda must revel in delight for having so significantly changed the course of history.[9] These factors, together with a sense of ethos—a

---

[7] David Rapoport, "Terrorism," in Mary Hawkesworth and Maurice Kogan, eds., *Routledge Encyclopedia of Government and Politics*, vol. 2 (London: Routledge, 1992), 1067.
[8] Audrey Kurth Cronin, *Ending Terrorism: Lessons for Defeating al-Qaeda* (London: IISS, Adelphi Paper 394, April 2008), 24.
[9] Bruce Hoffman, "A Counterterrorism Strategy for the Obama Administration," *Terrorism and Political Violence, 21: 3*, (2009), 360.

cultural philosophy expressed by its continued ability to operate and recruit—continue to energize the al-Qaeda insurgency.

COIN in Afghanistan- General McCrystal's Vision

The will of the Afghani people is at the heart of General Stanley McCrystal's Commander's Counterinsurgency Guidance. In 2009, McCrystal referred to the war in Afghanistan as a conflict that will be "won by persuading the population, not by destroying the enemy."[10] He said that "ISAF [International Stabilization Force Afghanistan] must operate differently. The Afghan people have paid the price, and the mission has been put at risk."[11] McCrystal emphasized in his Commander's Assessment that "our strategy cannot be focused on seizing terrain or destroying insurgent forces; our objective must be the population."[12] This new strategy underscored that the coalition has redefined the character of the fight in Afghanistan. McCrystal's strategy acknowledged that it was no longer a "cyclical, kinetic campaign based on a set fighting season," but rather, the ISAF's center of gravity should be the will and ability to provide for the needs of the population. [13] As such, civilian casualties and collateral damage to residential areas must be minimized with all necessary precaution. Non-kinetic operations correspond perfectly with this vision by offering methods of targeting the adversary at the heart of its operations, especially in its ability to effect communications, command,

> *"ISAF is a conventional force that is poorly configured for COIN, inexperienced in local languages and culture, and struggling with challenges inherent to coalition warfare. These intrinsic disadvantages are exacerbated by our current operational culture and how we operate."*
> *General McCrystal,2009*
> (Commander's Initial Assessment, 1-2.)

[10] Stanley McCrystal, "ISAF Commander's Counterinsurgency Guidance, 2009, 1.
[11] Stanley McCrystal, "Commander's Initial Assessment," 30 August 2009, 2-12.
[12] McCrystal, "Commander's Initial Assessment," 30 August 2009, 1-1.
[13] Ibid, 2-3.

and control, while at the same time minimizing kinetic distress to the population.

Making the Case for Non-Kinetics in Afghanistan

The overwhelming power of coalition strength, when wielded with capable planning and weaponry, is intended to eliminate or reduce insurgent influence in the region. But, ironically, that same great power has the potential to *strengthen* the insurgent's sense of resolve, which is magnified every time a coalition munition goes astray. For instance, in mid-February 2010, NATO and Afghani forces engaged in a significant push through the Marjah region as part of a larger offensive meant to shatter the Taliban stronghold in southern Afghanistan. Press reported that two US missiles struck a house where 12 civilians were killed—"half of them children," it was quick to point out[14]. In small print, one usually finds details of the attack, which point to more truth than rhetoric. In this case, the news piece later mentioned that "three Taliban fighters were in the house at the time of the attack."[15] The point here is that kinetic coalition efforts may be succeeding in eliminating adversary targets of opportunity, such was case with the three Taliban fighters in the house on 16 February. However, more damage was likely caused by anti-Coalition propaganda that incessantly surrounds such kinetic operations.

[14] Associated Press, "Civilian Death Toll Rises in Afghanistan," 16 February 2010, http://www.foxnews.com/story/0,2933,586084,00.html/, (27 February 2010).
[15] Ibid.

According to General McCrystal, "civilian casualties and collateral damage to homes and property resulting from an over-reliance on firepower and force protection have severely damaged ISAF's legitimacy in the eyes of the Afghan people."[16] In his 2009 Assessment, McCrystal concluded that "ISAF is not adequately executing the basics of COIN doctrine."[17] As a result, McCrystal charged ISAF to change its operational culture so as to put the Afghan people first. Such focus fits an increased emphasis on non-kinetic operations in order to reduce the kinetic face of coalition operations.

Naturally, there will be some kinetic operations that simply cannot be replaced by non-kinetic means. A mindset of *replacement* is not the nature in which non-kinetics are intended to operate. Instead, non-kinetic options such as those that affect the adversary's use of space and cyberspace, should be considered critical *adjuncts* to kinetic power. Likewise, ISAF planners should to recognize important non-kinetic options during strategic initiatives such as the February 2010 Marjah Offensive.

A security advising team suspected the Regional ANP chief to be corrupt. Following many attempts to aid a change in behavior, the security team built a case to take to the Provincial leadership. A non-kinetic operation revealed evidence confirming the corrupt Chief. He was removed and replaced with a loyal, diligent leader who improved the Provincial Afghan justice system. Although the process took time, one non-kinetic operation empowered leaders to take action and ultimately protect the population from an internal malignant actor.

Likewise, kinetics in Iraq have accorded American forces less-than-reputable press. This bolsters the argument for more non-kinetic options in the area. A recent example surfaced on 5 April 2010 when the leaked footage of an AH-64 APACHE gunship showed a 2007 mission which killed a dozen in Baghdad, including two Reuters reporters. This kinetic operation, now

[16] McCrystal, Commander's Initial Assessment, 30 August 2009, 2-10.
[17] McCrystal, Commander's Assessment, 2-11.

visible to the public, lawfully targeted a confirmed insurgent group; but the AH-64 APACHE crew had no way of knowing that two Reuters reporters, who appeared to be insurgents themselves, were imbedded with the group.[18]

Though these men appeared to be lawful combatants and legal targets under the Law of Armed Conflict, incidents such as this call to question the rules of engagement under such circumstances. "I believe that if those killings were lawful under the rules of engagement, then the rules of engagement are wrong, deeply wrong," said David Schlesinger, Reuters' editor in chief.[19] He went on to say that the fliers in the video act "like they are playing a computer game and their desire is they want to get high scores by killing opponents."[20] Additionally, kinetic operations such as this—where civilian casualties are involved, or mission lawfulness is questioned—causing backlash from some news agencies that twist the reality of war. Such was the case when another news agency interpreted the event in which they reported as a "brutal slaying of a group of civilians."[21] In this case, kinetic operations left room for deceptive blame, anti-American propaganda, and misleading wartime rhetoric—all at the expense of American efforts to make lives better in Iraq. Kinetic planners and operators need more options; the solution lies in the availability of more non-kinetic choices.

However, USCENTCOM planners have a challenge. Today there are trends which blur traditional lines of fighting. For example, technology now allows warfighters to integrate kinetic and non-kinetic capabilities into an all-in-one system that integrates sensor, processor,

---

[18] David Alexander and Phillip Stewart, "Leaked U.S. Video Shows Iraq Deaths, Including Reuters Staff," Reuters. 5 April 2010, http://www.reuters.com/article.idUSTRE6344FW20100405/, (accessed 25 April 2010).
[19] Alexander, "Leaked U.S. Video," 1.
[20] Alexander, "Leaked U.S. Video," 1.
[21] Henry Hunter, "Leaked APACHE Gunship video Iraq 2007: Two Reuters Reporters Killed Updated," 7 April 2010, http://worldnewsvine.com/2010/04/leaked-apache-gunship-video-iraq-2007-two-reuters-reporters-killed/, (accessed 25 April 2010).

distributor, and kinetic or non-kinetic shooter-penetrator on a single aircraft. Perhaps even more attractive to the planner and operator is a distributed set of multiple aircraft that share all this information and can coordinate tasks without duplication of effort in a fractionated system.[22] If non-kinetic operations through the use of advanced technology and continued control of cyberspace can allow the US to achieve such capacity, one can hope there will be a greater degree of survivability.

If the aforementioned trends for combined-role aircraft continue, one could argue that the traditional bomber, fighter, or intelligence collection aircraft might eventually disappear. However, Lieutenant General Deptula cautions that in the face of traditional Air Force terminology, these do not constitute multirole aircraft, but "rather a more advanced integrated mission composable approach."[23] In this so-called *composable approach,* non-kinetic operations have the opportunity to thrive. The integration of multiple functions on single platforms makes reliance on linking to other platforms less critical. Therefore, the composable approach is more viable in an environment where advanced jamming and information denial operations are at the adversary's fingertips.

One such non-kinetic environment was discernible in the 2006 Israeli-Hezbollah Conflict. In this conflict both sides demonstrated non-kinetic capability, but with varying resolve. The following section explores the implications of non-kinetic operations to one of the United States' most significant allies in the Middle East—Israel.

[22] Fulghum, "Military Tech, Organizations Will Merge," 1.
[23] Fulghum, "Military Tech, Organizations Will Merge," 1.

A Comparison: Israeli Cyber Attack Force Declared

Like the United States, Israel is a leader in the use of non-kinetic warfare. In 2006, during its war with Hezbollah, strategic national security interests drove non-kinetic operations to the top of Israel's priorities. Heading the list was denial of the adversary's use of cyberspace by any means necessary, including radiofrequency jamming and kinetic operations against cyber targets.[24] It is also possible that Israel planned for and may have engaged in offensive cybernetic operations. Unlike the first two means, capacity for offensive cyber operations are highly sensitive and generally covert. Indeed, classification concerns will remain an issue. Hence, the conduct of offensive cyberspace operations requires careful consideration and preparation before employment of such sensitive means.

In early February 2010, the Israeli Defense Forces officially sanctioned cyber-attack as a specified mission of the Israeli Defense Forces.[25] Emphasizing these modern priorities, Major General Amos Yadlin, Chief of Military Intelligence, claimed that "Fighting in the cyber dimension is as significant as the introduction of fighting in the aerial dimension in the early twentieth century."[26] In order to confront the cyber threat, computer networks are to be exploited by hacking into databases or carrying out sabotage with malicious software. In addition to offensive missions, the Israeli Defense Forces openly emphasizes the

---

[24] Anthony H. Cordesman and William D. Sullivan, *Lessons of the 2006 Israeli-Hezbollah War*, (Washington, D.C.: Center for Strategic and International Studies, 2007), 140; Paul McLeary, "High-Tech Weapons Are Standard Issue for Insurgents," *Aviation Week*, 13 February 2008. http://www.aviationweek.com/aw/generic/story_generic.jsp?channel=dti&id=news/DTIINSURTECH.xml&headline=high-Tech%20Weapons%20Are%20Standard%20Issue%20For%20Insurgents/, (accessed 26 April 2010). David Eshel, "Hezbollah's Intelligence War," *Defense Update*. http://defense-update.com/analysis/lebanon_war_1.htm/, (accessed 26 April 2010).

[25] Ibid.

[26] "Israel Adds Cyber-Attack to IDF" *Defense Tech*, 11 February 2010, http://defensetech.org/2010/02/11/israel-adds-cyber-attack-to-idf/, (accessed 15 February 2010).

use of cyberspace for the gathering of vital intelligence. Yadlin stated the "cyber warfare field fits well with the state of Israel's defense doctrine. This is an enterprise that is entirely blue and white [Israeli] and does not rely on foreign assistance or technology."[27] Yadlin's words remind the American audience that capability for independent action remains extremely important to the Israeli Defense Forces.

> *"The potential exists here for applying force ... capable of compromising the military controls and the economic functions of countries, without the limitations of range and location."* Major-General Amos Yadlin, Israeli Chief of Intelligence. (*Defense Tech*, Feb 2010).

As seen in the 2006 Israeli-Hezbollah conflict, Hezbollah used such dissemination of propaganda to its advantage.[28] A Harvard University study asserted that Israel's defeat came not at the hands of Hezbollah, but rather that Israel was "victimized by its own openness."[29] The Harvard study concluded that Hezbollah's means of using cyberspace to exploit information worked. This compounds the problem of information sharing and highlights the emphasis of non-kinetics in modern warfare for adversaries and allies alike. Furthermore, such non-kinetic warfare is becoming a common tactic, and the rest of the world is taking note.

Israel's Non-Kinetic Influence with Regional Consequences

Considering the degree of emphasis Israel has placed on cyber-attack, one must consider what implications this move will have on its regional nemesis, Iran. Such overt emphasis on cyber attack may seem

---

[27] "Israel Adds Cyber-Attack to IDF," *Defense Tech*, 11 February 2010, 1 http://defensetech.org/2010/02/11/israel-adds-cyber-attack-to-idf/, (accessed 27 February 2010).
[28] Matt Matthews, "The Israeli Defense Forces Response to the 2006 War with Hezbollah," *Military Review*, Jul/Aug 2009, Vol. 89 Issue 4.
[29] Marvin Kalb and Carol Saivetz, "The Israeli-Hezbollah War of 2006: The Media as a Weapon in Asymmetrical Conflict," KSG Faculty Research Working Paper Series RWP07-012, February 2007, 1.

quite threatening considering Israel's prior performance—it can and *will* use force when deemed necessary. Such has been the case time and again, garnering Israel a reputation for action. In 1967 Israel initiated pre-emptive surprise strikes on the Egyptian Air Force in the Six-Day War.[30] In 1981 Israel took the initiative with Operation Opera, when a surprise air strike destroyed the Osirak nuclear reactor in Iraq.[31] And in 1982 in Operation Peace for the Galilee, Israel invaded Lebanon.[32] These three examples illustrate Israel's willingness to act—serious events to consider if Israeli now holds non-kinetic options in its quiver. An impending non-kinetic threat from Israel could be a potential point of friction between it and Iran, especially if Iranian President Mahmoud Ahmadinejad continues to seek legitimacy through regional influence and nuclear power. Recent actions by Iran have pointed toward a quest for empowerment.[33] For the past year, a more moderate US policy toward engagement with Iran has not provided plausible verification that Iran could be discouraged from obtaining nuclear weapons. A regional asymmetric threat in the form of Israeli non-kinetic operations could become the proximate cause that unleashes the Iranian nuclear potential.

Could Israel's aggressive cyber-attack mission act as a catalyst for the Iranian nuclear program? If Iran perceives the Israeli cyber force as a serious asymmetric threat to Iranian security, it could vindicate Iranian leaders—at least in their minds— to hasten the pace toward nuclear

---

[30] "In 1967 Israel was aware of an impending attack by Egypt, to be assisted by Jordan, Iraq and Syria, and won a brilliant and total victory in only six days…largely because they launched a pre-emptive attack on the Arab air forces…" David Robertson, *The Routledge Dictionary of Politics*, (New York, N.Y.: Routledge, 2003), 22.

[31] McCormack claims secret Iraqi weapons facility confirms 1981 Israeli suspicion. Timothy L. McCormack, *Self-Defense in International Law: The Israeli Raid on the Iraqi Nuclear Reactor*, (New York, NY: St. Martin's Press, 1996), 18.

[32] Richard A. Gabriel, *Operation Peace for Galilee: The Israeli-PLO War in Lebanon*, (New York, N.Y.: Hill and Wang, 1984).

[33] Patrick Cronin, "Iran on the Threshold: From Engagement to Comprehensive Containment," *The DC*, 15 February 2010, http://dailycaller.com/2010/02/15/iran-on-the-threshold-from-engagement-to-comprehensive-containment/, (accessed 27 February 2010).

weaponization. Israeli strategy has no doubt taken this possibility into consideration, yet it has made the decision to go forward with significant non-kinetic programs. If, in the Israeli calculus, non-kinetic cyber operations are worth the possibility of a nuclear response by a state committed to its destruction, do non-kinetic cyber operations rise to the level of nuclear weapons in strategic importance? With this question, it is useful to reassess the role of non-kinetic operations. Though so different from their kinetic brethren, they may have a unique compellence or deterrence quality all their own.

In summary, today's security environment in Afghanistan calls for minimized collateral damage; a scenario that begs increased space and cyberspace operations as an alternative to kinetic warfare. Additionally, at a higher strategic levels of war, it is important for strategists and active theater planners to consider the deterrent and compellent qualities of non-kinetic operations. Akin to an Israel-Iran scenario, strategic implications of non-kinetic potential must be balanced with strategic intent. Finally, if non-kinetic capabilities enable a strategic effect, one must consider the varying interpretations of what might be considered an *act of war*.

Chapter 3

Doctrine, Authorities and Legalities

Here in America we are descended in blood and in spirit from revolutionists and rebels - men and women who dare to dissent from accepted doctrine. As their heirs, may we never confuse honest dissent with disloyal subversion.
– Dwight D. Eisenhower

Joint Publication Doctrine

Non-kinetic operations are not well grounded in existing doctrine. Space operations have a foundation, but cyber operations remain an emerging field without a stand-alone doctrine. Cyberspace is a realm where idiom and ideology have not yet met.

According to Joint Publication 3-14, advances in space systems have increased the importance of space power to the warfighter and American national interests.[1] This doctrine emphasizes that space superiority ensures freedom of action and use of space operations to influence an adversary in ways not afforded to kinetic options.

JP 3-14 states that when directed, space control operations should deny freedom of action to an adversary. Such denial can be accomplished through offensive and defensive operations to gain and maintain space superiority. To utilize space and cyber offensive operations to their fullest, both deliberate and crisis action planning are conducted. The Commander, US Strategic Command (CDRUSSTRATCOM) is responsible for integrating and synchronizing Department of Defense space capabilities to ensure the most effective use of space resources. "During mission execution, CDRUSSTRATCOM will retain combatant command (authority) of assigned space forces and where appropriate, transfer operational control or tactical control with

[1] JP 3-14, *Joint Doctrine for Space Operations*, 9 January 2009, vii.

Secretary of Defense approval to the JFC depending upon the nature of the operation and the specific space capability."[2]

Space and cyberspace doctrine must be constructed with consideration for the information realm in which both are inherently connected. As such, the United States has made it a priority to maintain information superiority. US Joint doctrine defines information superiority as "the operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying any adversary's ability to do the same."[3]

> *"There is a capability from CONUS, which has been chopped to Multi-National Forces-Iraq (MNFI) since 2004 that conducts cyber operations, and there are people who have been detailed to perform cyber operations, but there is no cyber coordinating authority below USSTRATCOM or instead of USSTRATCOM; it does not exist."*
> *Brig Gen Michael Carey*

Joint Publication 3-14 allows for a space coordinating authority (SCA) to be delegated from the Combatant Commander to whomever he or she chooses. USCENTCOM has decided that the Combined Forces Air Component Commander (CFACC) be that person.[4] Other Geographic Combatant Commands have not delegated space coordinating authority below the four-star level.[5] *Only* USCENTCOM has this construct; however, the Commander does not have overarching cyberspace authority. There is no such mandate stated in law or doctrine. The only regulations that exist for cyberspace coordination are the Unified Command Plan (UCP), execution orders (EXORDS), and Countering Adversary Use of the Internet (CAUI) guidance.

---

[2] JP 3-14, *Joint Doctrine for Space Operations*, 9 January 2009, xi.
[3] US Joint Chiefs of Staff, *Information Operations,* Joint Publication 3-13 (Washington DC: US Joint Chiefs of Staff, February 13, 2006), GL9.
[4] Carey, interview, 13 May 2010.
[5] Carey, interview, 30 November 2009.

For cyberspace operations, authoritative complications arise due to CFACC planner's separation from the Afghanistan theater of operations. According to Brigadier General Michael Carey, the CFACC planners, who are situated in Al Udeid, are *physically* too far from the planning elements resident in Afghanistan. Carey argues that though non-kinetic planners try to integrate the CFACC into their activities, coordination has not been efficient. Like most things in warfare, the cyber -kinetic coordination piece is a people problem; and even though cyber operations are not usually limited by geography, the people planning and operating them in war may be so limited. That is why the Air Component Control Element (ACCE) is utilized. However, the ACCE does not have necessary authorities. The ACCE Handbook confirms that the ACCE has no command authority; it especially does not carry the authority the CFACC has at the Al Udeid Combined Air Operations Center (CAOC).[6] Thus, the ACCE in Afghanistan as a relatively ineffective representative for non-kinetic operations.

So the question is this: If you have non-kinetic planners and operators placed in Afghanistan (and Iraq), do they have to come with authorizations that are recognized by the community? Presently, operators can get such authority for space operations. But they *cannot* get it for cyber, because there is no provision for it and JP 3-13 effectively fragments it. According to the current doctrine in JP 3-13, its direction is broadly strewn by design, as it essentially says that everybody should be able to do whatever they want with cyber and Information Operations.[7] Therefore, the crux of the problem is doctrinal, and the solution lies in clarifying authorities.

---

[6] Secretary of the Air Force, *Air Force Doctrine Document 2*, 3 April 2007, 71.
[7] JP 3-13, I-6.

A Call to Change Doctrine

If the crux of the problem is doctrinal, as the previous argument concludes, one must express precisely *what* needs changing and what process will best advance that doctrinal change. An assumption here is that codification of cyberspace operations doctrine will empower cultural change. Critically, however, when changing doctrine, a primary issue is *timeliness*. Doctrine always lags behind current trends. But doctrine is (ideally) informed by what is learned in practice, and best practice doctrine is informed by events in war.

This is the fundamental conundrum in the joint doctrine process. For doctrine to be changed, significant lead and lag time must be accepted for Joint Forces Command (JFCOM) to generate a useful product. For example, a typical doctrinal change would look something like the following: JFCOM studies an operation, captures its lessons learned, develops tactics techniques and procedures (TTPs), tests them in exercises and wargames, and ultimately molds joint doctrine.[8] Sometimes it takes years to mold doctrine.

Thus, there is no current non-kinetic doctrine for joint operations in cyberspace. The problem has been exacerbated by the command structure in Afghanistan. As General McCrystal took command at ISAF, an intermediate joint command being formed. Typically, whenever a new command is activated, initial guidance comes from joint doctrine. Training and structure are established as doctrine instructs. For instance, JP 3-13 tells the Intermediate Joint Command (IJC) how to structure Information Operations. Because doctrine states there are five pillars of Information Operations—Computer Network Operations (CNO), Electronic Warfare (EW), Military Deception (MILDEC), Psychological Operations (PSYOP), and Operations Security (OPSEC)—each is established and organized independently. Although JP 3-13 specifically

[8] Joint Pub 1-01, *Joint Publication System*, I-3.

describes and places computer network operations within the larger construct of IO, it is not consistent with how joint forces are actually operating. In reality, JP 3-13 acts against how US forces *should* operate, especially regarding the integration of space and cyber for effect. In essence, current doctrine stated in JP 3-13 describes how to fracture an organization.

The initial problem with JP 3-13, is that it was written when American forces were not very cyber savvy. While USSTRATCOM and cyberspace operators are still working on planning and execution nuances, joint operators are sharing best practices in real time and making organizational adjustments on the fly.

As a result, JP 3-13 reflects IO pillars that have since broken down. Responding to operational realities, General Kevin Chilton, Commander USSTRATCOM, has separated cyber from IO on the recognition that cyberspace is now an independent line of operation. Emphasis in war has changed the way IO is structured. Cyberspace operations play such a significant role they deserve their own identity, no longer subordinated under a generalized category of IO. Electronic warfare, as conceived in JP 3-13, has also been effectively separated from Information Operations because of its close ties to cyber and its many independent capacities. Reflective of Chilton's actions, one might argue that today's IO is better defined as a three-pillar system, where Operations Security (OPSEC), Military Deception (MILDEC), and Psychological Operations (PSYOP) reside, rather than the current five-pillar construct. Experience in non-kinetic operations in Iraq and Afghanistan have shown that the old divisions are more inhibiting than enabling and that a new structure that reflects current operational needs is required —a "slurry mix of non-kinetics regardless of where the 'trons' come and go," says Chilton's Deputy J3, Brig Gen Michael Carey. But doctrinally, JP 3-13 does not allow the joint community to do that.

JP 3-13 also prompts authority and liability issues. In practice, given that cyberspace is a line of operation, who works for whom? Where do they act, and how do they get what they need? In the case of Afghanistan and McCrystal's intermediate joint command, the only doctrinal choice was to starts with JP 3-13. Doing so created an organization that separates individuals into impractical stovepipes, fragments where they should act, and splinters the processes in which they are engaged.

In Afghanistan, McCrystal's non-kinetic organization resulted in the following fragmented construct: one non-kinetic effort at Camp Green, physically located away from HQ ISAF, and physically located away from the Intermediate Joint Command (IJC); and three separate locations in Kabul, which required cross-compound planning, making coordination cumbersome. This organizationally fractured construct has produced sub-optimized mission planning and poor communication.[9] Compounding the difficulties, secure phone communication via ISAF-Secret is not shared commonly across the world, all but guaranteeing that collaborative planning will be difficult.

Air Force Leads the Way

In the end, if doctrine can be changed to counter these problems, non-kinetic operations will be conducted more efficiently with better processes in place for multi-service contingency operations. But akin to early days of airpower, the following question requires an answer: Is the Air Force the right service to lead space and cyberspace doctrine? Although changing cyber doctrine is largely a strategic joint issue, an Air Force lead should not overshadow the fact that the other services have a significant role in non-kinetic efforts.

For example, Naval Chief Information Officer Robert Carey credits current space and cyber operations for pushing the Naval way of warfare

[9] Carey, interview, 30 November 2009.

forward. He praises efforts such as Operation GLADIATOR PHOENIX, the operation to operate in and defend the global information grid (GIG), for introducing new strategies to confront information technology's vulnerabilities. Thanks to the emphasis of non-kinetic warfare in Operation GLADIATOR PHOENIX, the Navy has outlined a "strategic transition to a new school of thought in Navy cybersecurity."[10] The recent founding of US Fleet Cyber Command/US Tenth Fleet, activated 29 January 2010, underscores necessity for an active cyber mission. The new command includes 44,000 personnel and 1,000 new cyber warriors.[11] Carey argues that such operations will nurture a cultural makeover within the Navy and will result in new non-kinetic conduct within naval defense and offensive capabilities.

The army has also embraced the benefits of Operation GLADIATOR PHOENIX and the establishment of a unified command dedicated to cyberspace. General Carter F. Ham, USA, commanding general, US Army Forces Europe and Seventh Army, maintains this is a historic time for the United States Army.[12] He specifically indicated the significance within the Army's signals community. Brigadier General Steven W. Smith, USA, the Army's chief cyber officer, underscored Ham's comments by noting the Army's contributions to major non-kinetic initiatives including the Comprehensive National Cyber Initiative (CNCI), the Defense Department Information Assurance Campaign Plan (DOD IACP), the establishment of the US Cyber Command (CYBERCOM), and Operation GLADIATOR PHOENIX. Smith added that the Army's focus is

---

[10] Amber Corrin, "Navy CIO Unveils New Strategies for Navy Cybersecurity," *Washington Technology*, 13 August 2009, http://washingtontechnology.com/articles/2009/08/11/fose-preview.aspx/, (accessed 15 February 2010).
[11] Fleet Cyber Command/Ten Fleet Public Affairs. "Navy Stands Up Fleet Cyber Command, Reestablishes U.S. 10th Fleet." 29 January 2010. http://www.navy.mil/search/display.asp?story_id=50954/, (accessed 25 April 2010).
[12] Henry S. Kenyon, "US Army Ponders Cyber Operations", *Signal*, 15 October 2009, 1.

to integrate efforts across the Army staff to "provide policy, oversight and guidance" for non-kinetic operations.[13]

Though army and naval planners have embraced non-kinetic options, a significant majority of the people actively conducting space and cyberspace operations are Air Force personnel in Air Force organizations. Additionally, the Air Force's traditional position at the forefront of technological developments in warfare makes the USAF appear to be the logical service to lead space and cyber non-kinetic warfare development and operations. With the potential for growth in these areas, one would expect a certain amount of inter-service positioning to lead the effort, and to an extent this has been the case. But even within the Air Force there is friction concerning acceptability and greater understanding of non-kinetic capabilities.

> *We're going to have to be ready to operate in a complex, chaotic information environment on the battlefield. Warfighters must improvise because war is unpredictable. General James Mattis, USMC, Commander, JFCOM (*Kenyon, *Signal, Oct 09).*

Intra-service conflict within the Air Force is not new. It was widely experienced during the early years of the Cold War between Bernard Schriever and Curtis LeMay, for instance. The strategic bombing zealots could not see the strategic benefit of the Intercontinental Ballistic Missile (ICBM). LeMay said the Air Force was wasting its resources putting so much effort into missiles and space.[14] For LeMay's purposes, these efforts were taking away precious time, money and attention from the advancement of the USAF' core competency—strategic bombing with advanced aircraft.

Fortunately, today's intra-service friction does not compare to that of the days of the Cold War, but the legacy continues. Resources spent

---

[13] Henry S. Kenyon, "US Army Ponders Cyber Operations", 1.
[14] Neil Sheehan, *A Fiery Peace in a Cold War: Bernard Schriever and the Ultimate Weapon* (New York N.Y.: Random House, 2009), 159.

on space and cyber are still viewed by some proponents of airpower as taking away from necessary maintenance and modernization of an aging air-based inventory. Nor do non-kinetic operations have the immediate and visceral impact of today's deadly precision kinetic strikes. Thus, it is understandable that kinetic warfare advocates within the Air Force have been slow to see the value in non-kinetic operations until they are submerged in the missions and see the results of space and cyberspace operations. Such Air Force leaders are not *against* the use of non-kinetic options. But they do not prefer such methods of warfare, especially because demands from other air-breathing missions have their full attention. Senior Air Force leaders are coming around, but so far they have not had the resources to support the full array of traditional missions *and* move strongly to new competencies.

Ultimately, the Air Force is best suited to lead cyber for many of the same reasons the Air Force has been looked to as the lead contributor to space for the past 50 years. Although cyberspace touches every service, like the space domain, cyber is becoming an important USAF legacy. According to Lieutenant General David Deptula, there are three reasons for this growing legacy. First, cyber is giving traditional Air Force assets the "ability to rapidly compress and decompress data due to advancing computing speed."[15] Second, Air Force systems, more than any other service have the "ability to transmit this data using very clever means—like transmitting only the parts of a video or radar picture that have changed."[16] Third, the Air Force has the "ability to bring all these technologies onto one platform."[17] Evidence of this emergent legacy is seen in daily Remotely Piloted Aircraft (RPA) missions throughout the USAF. Together, these advances are amplifying the speed of information to the warfighter and decision maker alike, in the process changing the

[15] Fulghum, "Military Tech, Organizations Will Merge," 1.
[16] Quoted in Fulghum, "Military Tech, Organizations Will Merge," 1.
[17] Quoted in Fulghum, "Military Tech, Organizations Will Merge," 1.

way future aircraft are designed, the structure of USAF organizations, and even long-term service norms. Such norms include changes in cultural habits connected to collection, analysis, and distribution of war-time information.

As noted earlier in this study, there is a large degree of centrality and inseparability between space and cyberspace. The United States Air Force provides the adhesive binding the two missions in the ultimate joint fight. It does this in three ways: first, the Air Force's global focus embraces cyberspace's enduring global capabilities; second, like the space domain, cyberspace is shared by other services, but requires managed development in the service with just the right custodial supervision to make it excel with forthcoming technologies into the future; third, the Air Force routinely uses cyberspace in daily operations supportive of not only its own organic missions, but in support of Air Force contributions to the joint and coalition environment.

Additionally, Deptula says that cyber warfare is a part of the intelligence, surveillance, and reconnaissance future. "A big part of the job in exploiting operations in cyberspace entails computer network exploitation."[18] For this reason, exploitation of cyberspace is a key mission set of 24th Air Force with Air Force ISR Agency capabilities being vital to that mission. They are so important that 24th Air Force has established a group of about 400 people in direct support of cyberspace exploitation.[19]

Legalities

According to the 2008 Unified Command Plan, USSTRATCOM has the roles and responsibilities to conduct, execute, and operate space and cyber missions, to include the forces necessary to do so.[20] This authority is not delegated or assigned to the Geographic Combatant Commands

[18] Quoted in Fulghum, "Military Tech, Organizations Will Merge," 1.
[19] Fulghum, "Military Tech, Organizations Will Merge," 1.
[20] Unified Command Plan (UCP), December 2008

(GCCs), although they have been undertaken by the GCCs as an *implied* as opposed to *specified* activity.[21] The USCENTCOM Commander, General Petraeus, as well as his component commanders, believe that he has the inherent authority, inherent right, and obligation to use all capabilities to prosecute the war. "However, when conducting cyber operations garnering requisite legal authority is problematic," according to Brigadier General Michael Carey, Deputy Director, Global Operations, United States Strategic Command.[22] This was the case recently when USCENTCOM attempted cyber operations against an insurgent target. The Department of Justice precluded the operation because USCENTCOM did not yet have the legal authorization to do so in that case.[23]

As of February 2010, the best example of legal friction for non-kinetic warfare is being dealt from the highest levels of government. Operation GLADIATOR PHOENIX is the named operation to operate and defend the GIG.[24] In February 2010, the issue with this critical operation involved some constituencies in Washington D. C. that wanted to *restrict* that operation to an area of hostilities.[25] However, United States and coalition networks are under attack all the time, and attacks come from anywhere. In many cases, if one were to restrict the application of force to the area of hostilities, that force would be simply ineffective. The concern of some in Washington is that they do not want non-kinetic offensive action to be taken within the United States. But what if the adversary is conducting cyberspace operations from the United States? What if the adversary is conducting cyberspace

---

[21] Carey, interview, 30 November 2009.
[22] Carey, interview, 30 November 2009.
[23] Carey, interview, 30 November 2009.
[24] Henry S. Kenyon, "US Army ponders Cyber Operations," 1.
[25] According to USSTRATCOM discussions with officials in Washington D.C., there are political opponents to Operation GLADIATOR PHOENIX who desire restrictions on the operation in order to further protect American freedom of speech rights. Carey, interview, 30 November 2009.

operations from Singapore, from Somalia, or from France? Are those same concerned parties in Washington telling American forces that they cannot attack a hostile network if it does not exist in Iraq or Afghanistan? Carey adds, "If the adversary is leveraging the protections afforded by the First Amendment, effectively using our rights against us, then we have to go to the Department of Justice for assistance."[26] For all of these reasons, the argument for restricting non-kinetic operations to a declared hostile area falls apart fast. The legal operating areas of cyber should not be limited to an area of hostility, but rather must allow pursuit of hostile actors with hostile intention wherever they may be.

In response to this scenario, Brig Gen Michael Carey states, "I am not against the Geographic Combatant Commander (GCCs) executing the mission, but they don't have the command and control, and they don't have the strategic situational awareness afforded to USSTRATCOM."

A Question of Command Authority

If cyberspace authority is given to the commander in USCENTCOM, there are still strategic-level non-kinetic operations being conducted from USSTRATCOM of which the USCENTCOM commander has no awareness. Therefore, significant problems can arise if two separate entities operate similar non-kinetic effects without coordination or proper risk assessment. The problem accelerates when USCENTCOM conducts minor operations that unintentionally disclose capability or intent at an operational or strategic level. These implications could have significantly adverse strategic effects for space and cyber operations happening at national security levels of higher interest that those in the USCENTCOM region. An additional consideration is that the GCCs do not have control of all non-kinetic assets, which often results in sub-optimized operations. For example, a capability coming out of CONUS, supporting an operation

[26] Carey, interview, 30 November 2009.

in Iraq can also support an operation in the PACOM. But not if it is commanded from CENTCOM. One *could* exercise command from CENTCOM, but how efficiently one plans the apportionment of human resources becomes the *true* limiting factor. The most limiting factor for non-kinetic operations is not the platforms, nor is it the apertures for space control. It is the people.

A Call for Clear and Appropriate Doctrine and Authorities

The preceding arguments indicate the need for clarification of necessary authorities in active theaters. It is thus recommended that joint doctrine mature the necessary command authorities through the development of non-kinetic authority and cyberspace doctrine. This recommendation does not preclude the need for changing authorities for cyberspace operations, but it does recommend the need for *re-enforced* authorities by the Geographic Combatant Commanders. Due to the global nature of space and cyberspace operations, such assets and missions cannot be restricted or limited to the area of hostility. This scenario was demonstrated in recent debates throughout Washington, especially in Congress and echoed in the halls of the Pentagon.[27] USJFCOM will be responsible for developing such doctrine, but as of the closing date of this study, no such doctrinal cyberspace authority exists.

[27] Carey, interview, 30 November 2009.

Chapter 4

Developing Non-Kinetic Senior Leaders: A Call for Expertise

Education is a lifelong experience. Experience is a lifelong education. Education plus experience equals expertise.

-- Michael Bugeja

The United States Air Force argues that it fights in air, space and cyberspace. But when it comes to naming space control experts in CENTCOM there are none above the grade of Lieutenant Colonel. In this theater, the DIRSPACEFOR is typically a space expert, but when the DIRSPACEFOR continually depends on USSTRATCOM for advice, indications are that there is a lack of cyber expertise. "There are field grade officers who are exceptionally bright, but the Air Force has not raised them to be space and cyber experts yet," says Brigadier General Michael Carey.

"So if you say 'name the fighter guy in theater', got it. 'Name the infantry guy', got it. 'Name the SpecOps guy in theater', got it. 'Name the cyber guy', and you come up empty."
Brig Gen Carey, DJ-3, USSTRATCOM

Cross pollination of expertise is the current concept. But because cyber operations are relatively new, there are not enough Air Force personnel with space *and* cyberspace background. There are those in lower grades, but they have been unable to influence operations sufficiently to produce significant effects.[1] Therefore, the USAF must institute a robust program aimed at developing enough capable officers in the field of space and cyberspace operations to populate higher ranking positions. Despite the urgency of the situation, some patience will be required to avoid hasty decisions by

[1] Carey, interview, 30 November 2009.

the Air Force's space and cyber non-kinetic community. Leaders must realize is that it will take time to develop the necessary number of experienced cyberspace planners and operators. According to Brigadier General Michael Carey, the process could take up to eight years to reach maturity.

The ballistic missile community experienced a similar learning curve prior to the merging of the space and missile communities. The merger took approximately eight years to develop a healthy pool of experienced officers with a breadth of experience in both career fields.[2] Carey believes the education of space and cyberspace warriors will require a similar catch-up scenario that will take years to see tangible results.[3] As with the space-missile merger, the problem was a demographic issue. There simply were not enough senior officers with backgrounds in both career fields to populate critical Air Force leadership positions that required multiple proficiencies. Until the Air Force merged the career fields of space and missiles there were not enough mid-grade officers with expertise in both fields from which senior leaders could emerge.

Though the current Air Force pool of expertise in the areas of space and cyber is small, some senior leaders with experience in both believe the change may be smoother than General Carey expects. Colonel Stephen Tanous, former USCENTCOM DIRSPACEFOR, is one of these experts. According to Tanous, "there are more parallels between the planning, C2, and execution of space and cyberspace forces than there were between space and missiles at the time of the space-missile merger."[4] Tanous asserts that at the time of the merger the ICBM community was already a very structured operational entity while space

---

[2] Carey interview, 30 November 2009.
[3] Carey interview, 30 November 2009.
[4] Col Tanous is a former Director of Space Forces (DIRSPACEFOR) at CENTCOM's Combined Air Operations Center, Al Udeid Air Base, Qatar. Colonel Stephen Tanous (Commandant, Squadron Officer School, Maxwell AFB, AL), interview by the author, 23 February 2009.

was much less further along the path to becoming an operational activity. But cyber has many more similarities to space; the C2 structures that have been established have much more in common as a result of the interdependence of the space and cyber communities as well as the maturation of C2 structures for both under USSTRATCOM over the last eight years, presenting fewer impediments to integration. For example, the command and structure of both space and cyberspace are designed to provide effects in a rapidly changing environment; ICBM operations are much more deliberate and measured by design, reflecting a relatively stable operational environment.

Additionally, the cadre of cyber and space operators are more likely to have a common mindset. For example, a space operator located at Schriever Air Force Base controlling satellites has a perspective and approach more akin to that of the cyber operator controlling operations via a terminal in Texas than either might have to an ICBM operator in the missile fields of Malmstrom Air Force Base. It is this outlook that defines the non-kinetic warrior, and an approach that many kinetic planners and operators do not yet fully comprehend.

A Cultural Change

Another issue critical to developing the population of experts in space and cyber operations involves a shift in cultural mentality. This may be one of the most important to the overall integration of space and cyber operators as they evolve into senior Air Force leaders. The attitude change that should occur involves seeing the value in allowing senior space officers to take responsibility in active theaters for non-kinetic operations. Currently, space officers are dissuaded from leaving a home-station command to serve in the capacity of a cyber advisor in the USCENTCOM AOR. However, if the approach were more encouraging of this broadening effort, the Air Force would see significant growth in the space-cyberspace expertise population. Unfortunately, senior officers are considered *too valuable* in positions they currently hold, and often are

not allowed to deploy.[5] If a greater value were placed on a space-cyber exchange and senior officers could go forward for say, six months, these experienced leaders would be much more valuable to the Air Force in the long term. These officers would experience how to apply the integration of space and cyber in time of war; a time that desperately demands innovation.

Expertise in space and cyberspace operations is only part of the equation for senior leaders in active theaters. Another significant point is the value of social and cultural understanding of non-kinetic warfare versus the adversary. Understanding the insurgent's social and cultural composition is critical. According to anthropologist Montgomery McFate, a lack of such understanding has strategic implications for American efforts in the area. McFate blames cultural ignorance of American leadership for hampering progress in Iraq. One example was the Bush administration's refusal to allow Ba'athist party members to serve in the new government.[6] Another example stresses the need for understanding both insurgent's cultural and technological networks. For many insurgents the tribal network has become the "backbone of the insurgency," according to McFate.[7] Coalition military leaders must consider these norms in concert with non-kinetic planning at the strategic, operational, and even tactical levels of war.

Martin Clemis gives credit to the newest US Army/Marine Corps counterinsurgency manual for calling attention to the value of cultural and social understanding in non-kinetic warfare.[8] Clemis applauds recent efforts and encourages future use of cultural awareness when training America's senior military decision makers. He approves of the

---

[5] Tanous, interview, 23 February 2010.
[6] Montgomery McFate, "Does Culture Matter? The Military Utility of Cultural Knowledge," *Joint Forces Quarterly 38* (Summer 2005), 44.
[7] McFate, "Does Culture Matter?," 43.
[8] Martin G. Clemis, "Crafting Non-Kinetic Warfare: The Academic-Military Nexus in US Counterinsurgency Doctrine," *Small Wars & Insurgencies*, 20: 1(2009), 160.

emphasis placed on expertise through scholarship toward developing "non-kinetic prescriptions for battling insurgency."[9]

Recommendation: A Call for Experts

The problem is not simply an organizational problem, but also one of expertise. This chapter makes an appeal for improved expertise, specifically within the active theaters of operations. This expertise will combine experience in non-kinetic warfare, to include space and cyberspace operations, in order to effectively achieve missions in Iraq and Afghanistan.

USSTRATCOM needs a forward representation, based in Afghanistan. Ideally this expert should hold the rank of colonel. This position shall be filled by a USSTRATCOM personnel who will not be assigned to USCENTCOM. When a theater commander starts affecting non-kinetic assets that transcend his area of operations, his planners and operators must consider what USSTRATCOM is doing and dictates of the national perspective.

Recognizing the need for combined space and cyber experts to USCENTCOM, Lieutenant General Keith B. Alexander, Commander, Joint Functional Component Command for Network Warfare (JFCC-NW), proposed establishing an Expeditionary Cyber Support Element.[10] In July 2009, USSTRATCOM formed a small team of combined space, cyberspace and Information Operations (IO) experts to deploy forward. Those IO experts selected to be part of the team combined experience in operational military deception (MILDEC), operational security (OPSEC), psychological operations (PSYOP) and Electronic Warfare. Additionally, Alexander

> *"We can deploy all the space smart people in the world, and they will not integrate with cyber people unless they are led to."*
> *Brig Gen Michael Carey*

[9] Clemis, "Crafting Non-Kinetic Warfare," 161.
[10] Carey, interview, 30 November 2009.

required the team be composed of an offensive cyber operator, a defensive cyber operator, and an intelligence officer. Since then, the unit has remained in the USCENTCOM area of responsibility and has been known as the USSTRATCOM Forward Integration Team (SFIT). The small team is headed by an O-6 and fills the expertise gap for cyber and space operations in CENTCOM. The aim of the team is to conduct planning and coordinate fires on those targets requiring kinetic or non-kinetic effects. Direct liaison with USCENTCOM planners will be critical to continued optimal use of space and cyberspace operations in Afghanistan. Limiting factors are still at play, such as inadequate facilities and infrastructure within theater. But Alexander's proposal of such a cyber support element gets the right people to the fight.

Meanwhile, acknowledging the theater's gap in space expertise, the DIRSPACEFOR at Al Udeid requested a large number of space experts be assigned to Afghanistan. However, Carey says that the issue is not about *more* space experts in theater, it is about *integration* of space and cyber experts and effects in theater.

Capitalizing on Private Sector Expertise

In addition to developing Air Force leadership proficiency in non-kinetics, joint and Air Force cyberspace operations should consider utilizing existing private-sector expertise. For the focus of this study, specific offensive and defensive proficiency with potential for actionable operational capability is the intended level of expertise. Though certainly of value to the cyberspace mission, private-sector computer scientists are not the target of this debate. Rather, private-sector expertise with direct potential for *operational* cyber warfare—in the Department of Defense sense—is the capability that the joint cyber community should advance. One such example might be seen in the Google-National Security Agency (NSA) agreement of 2010.

Nearly nine years after the 9/11 attacks, collaboration for cyberspace operations is finally taking shape. In January 2010, Google

stated that its system had been hacked by a string of month-long intrusions. Shortly after the attacks, Google contacted the NSA seeking its expertise and assistance in order to ensure better cyber security. According to Director of National Intelligence, Dennis C. Blair, the January 2010 Google attacks were a "wake up call" that required cyberspace expertise through a "collaborative effort that incorporates both the US private sector and our international partners."[11]

The partnership between Google and NSA, however, soon became controversial due to the delicate nature of the private-sector-government agency sharing of expertise and information. In this case, the world's largest Internet search company and the world's most powerful electronic surveillance organization teamed up to investigate cyber attacks.[12] The agreement expected to provide shared expertise and better security while allowing "the two organizations to share critical information without violating Google's policies or laws that protect the privacy of Americans' online communications."[13] For this reason, the Google-NSA partnership is at the heart of the sensitive balancing act between privacy and national security interests.

This agreement is central to the potential value of shared expertise between private and government cyberspace operations. Private sector expertise, together with enhanced cyber-savvy military leadership, will boost the future of non-kinetic operations through space and cyberspace capabilities.

In summary, the USAF needs to develop senior leaders whose expertise combines space and cyberspace operations. A renewed look at how the USAF trains and deploys their mid-grade through senior-level leaders should be a priority to ensure improved employment of non-kinetic capabilities. Additionally, USAF leaders must consider experts

---

[11] Ellen Nakashima, "Google to Enlist NSA to Help it Ward off Cyberattacks," *The Washington Post*, 4 February 2010, 2.
[12] Nakashima, "Google to Enlist NSA to Help it Ward off Cyberattacks," 1.
[13] Nakashima, "Google to Enlist NSA to Help it Ward off Cyberattacks," 1.

with wartime experience and use of private sector proficiency for truly enhanced non-kinetic operations in the future adversarial environments.

Conclusions

> *There is a great deal we can learn from this first war of the twenty-first century, but we cannot and must not make the mistake of assuming that terrorism is the only threat. The next threat we face may indeed be from terrorists, but it could also be cyber-war, a traditional state-on-state conflict or something entirely different.*
>
> *– Donald Rumsfeld*

The preceding analysis has demonstrated that cyberspace and space operations require several improvements in order to enhance non-kinetic operations. First, there is a need for clarification of non-kinetic authorities. Second, an update to joint cyberspace doctrine is required. Third, the United States Air Force must develop senior officers who are qualified to lead in both space and cyberspace capacities, particularly in wartime operations. In this regard, the United States Air Force must consider development of non-kinetic operations experts who have wartime experience in both space and cyberspace operations. Implementation of all three recommendations is necessary to improve the ultimate efficacy of non-kinetic operations.

If America's national strategy does not continue to adapt and evolve along with the technologically savvy adversary, other efforts will be for naught. Not only do the non-kinetic effects have to be linked to vital organs of the insurgent, but also, the larger strategy must wisely employ non-kinetic operations in a way that incorporates space and cyberspace capabilities with efficiency. According to Bruce Hoffman, the efficacy of coalition strategy will mirror the coalition's ability to think like a networked adversary, in order to foresee how the insurgent may react to a given scenario, supported by cyber and space resources.[1] Hoffman concludes, "This goal requires that the American national security

[1] Bruce Hoffman, "A Counterterrorism Strategy for the Obama Administration", *Terrorism and Political Violence, 21: 3*, (2009), 372.

structure in turn organize itself for maximum efficiency, information [expertise] sharing, and the ability to function quickly and effectively under new operational definitions."[2]

The continued need for defensive cyber and space capability is growing by the day. Dennis C. Blair, the director of national intelligence, in February 2010 warned the Senate Intelligence Committee, "Malicious cyber activity is occurring on an unprecedented scale with extraordinary sophistication."[3] To underscore the significance of defensive space and cyberspace awareness, a rare public cyber war game was exercised on 17 February 2010. Highest levels of American decision-makers were involved in the effort designed to highlight the nation's potential vulnerability in the event of a doomsday cyber attack. During the simulation, ten former White House advisors, the National Security Council and other top leaders acted in what many called uncharted territory. It was uncharted because the simulation included a simulated nationwide Internet crash, 60 million dead cell phones, massive electric grid failures, national financial failure, and commercial collapse. Together, these national security effects crippled America, leaving leaders in Washington virtually helpless. But this was just a drill.

The reality of non-kinetic threats looms broadly across America every day. The key to non-kinetic success in the USCENTCOM theater will be reliant upon the harnessing of kinetic options in an environment where non-kinetic capabilities may be the more optimal alternative. The vision to solve the non-kinetic problem must include clearly defined authority, tightly woven doctrine, and specialized non-kinetic expertise for execution.

---

[2]Bruce Hoffman, "A Counterterrorism Strategy for the Obama Administration", *Terrorism and Political Violence, 21: 3*, (2009), 372.
[3] Bob Drogin, "In a Doomsday Cyber Attack Scenario, Answers are Unsettling," *Los Angeles Times*, 17 February 2010.

BIBLIOGRAPHY

Arquilla, John and David Ronfeldt, ed. *Networks and Netwars*. Santa Monica, CA: RAND Corp., 2001.

Alexander, David and Phillip Stewart, "Leaked U.S. Video Shows Iraq Deaths, Including Reuters Staff." Reuters. 5 April 2010. http://www.reuters.com/article.idUSTRE6344FW20100405. Accessed 25 April 2010.

"Al-Qaeda Websites Hit by Western Cyber Attacks," *Daily Telegraph*, 22 Oct 2008. http://www.telegraph.co.uk/news/worldnews/asia/afghanistan/3237930/Al-Qaeda-websites-hit-by-Western-cyber-attacks.html. Accessed 15 March 2010.

Associated Press. "Civilian Death Toll Rises in Afghanistan." 16 February 2010. http://www.foxnews.com/story/0,2933,586084,00.html.

Brafman, Ori and Rod A. Beckman, *The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations.* New York: Penguin Group, 2006.

Bugeja, Michael. Email correspondence with author, 30 March 2010.

Carey, Michael J. Interview with author, 30 November 2009.

Chilton, Kevin. "Cyberspace Leadership: Towards New culture, Conduct, and Capabilities." *Air & Space Power Journal*, Vol. XXIII, No. 3, Fall 2009, 7.

Claburn, Thomas. "Google Cyberattack linked to Two Chinese Schools." *Information Week*, 19 February 2010.

Clausewitz, Carl von. *On War*. Edited and translated by Michael Howard and Peter Paret. Princeton, N.J.: Princeton University Press, 1984.

Clemis, Martin G. "Crafting non-kinetic warfare: the academic-military nexus in UScounterinsurgency doctrine." *Small Wars & Insurgencies*, 20: 1(2009), 160 — 184.

Coleman, Kevin. "What Constitutes an Act of Cyber War?" *Defense Tech,* 18 June 2008. http://defensetech.org/2008/06/18/what-constitutes-an-act-of-cyber-war/.

Cordesman, Anthony H. and William D. Sullivan. *Lessons of the 2006 Israeli-Hezbollah War*. Washington, D.C.:Center for Strategic and International Studies, 2007.

Corrin, Amber. "Navy CIO Unveils New Strategies for Navy Cybersecurity." *Washington Technology*, 11 August 2009. http://washingtontechnology.com/articles/2009/08/11/fose-preview.aspx.

Crampton, Jeremy W. *The Political Mapping of Cyberspace*. Chicago, I.L.: The University of Chicago Press, 2003.

Cronin, Patrick. "Iran on the threshold: From engagement to comprehensive containment." *The DC*, 15 February 2010. http://dailycaller.com/2010/02/15/iran-on-the-threshold-from-engagement-to-comprehensive-containment.

Drogin, Bob. "In a Doomsday Cyber Attack Scenario, Answers are Unsettling." *Los Angeles Times*, 17 February 2010.

Eisenhower, Dwight D. Speech, Columbia University, 1954. http://dailytext.org/men-quotes/here-in-america-we-are-descended/. Accessed 25 April 2010.

Eshel, David. "Hezbollah's Intelligence War." *Defense Update*. http://defense-update.com/analysis/lebanon_war_1.htm/. Accessed 26 April 2010.

Fleet Cyber Command/Ten Fleet Public Affairs. "Navy Stands Up Fleet Cyber Command, Reestablishes U.S. 10th Fleet." 29 January 2010. http://www.navy.mil/search/display.asp?story_id=50954. Accessed 25 April 2010.

Freeman, Linton. *The Development of Social Network Analysis: A Study in the Sociology of Science*. Vancouver: Empirical Press, 2004.

Fulghum, David A., "Military Tech, Organizations Will Merge," *Aviation* Week, 13 April 2010. http://www.aviationweek.com/aw/generic/story_channel.jsp?channel=defense&id=news/asd/2010/04/13/02.xml. Accessed 25 April 2010.

Gabriel, Richard A. *Operation Peace for Galilee: The Israeli-PLO War in Lebanon*. New York, N.Y.: Hill and Wang, 1984.

Gladwell, Malcolm. *The Tipping Point*. New York: Little, Brown and Co., 2002.

Goldman, Emily O. *National Security in the Information Age*. Portland, O.R.: Frank Cass Publishers, 2004.

Guare, John. *Six Degrees of Separation.* Stage play. New York, N.Y.: Dramatists Play Service, Inc., 1990. Premiered Mitzi E. Newhouse Theater, New York City, NY, 16 May 1990.

Hoffman, Bruce. "A Counterterrorism Strategy for the Obama Administration." *Terrorism and Political Violence*, 21: 3, 2009, 359 — 377.

Holt, Thaddeus. *The Deceivers.* New York, NY: Scribner, 2004.

Huisman, Mark, and Maritje Van Duijn. "Software for Social Network Analysis." In *Models and Methods in Social Network Analysis*, edited by Peter Carrington, John Scott, and Stanley Wasserman, 270-316. New York, N.Y.: Cambridge University Press, 2005.

Hunter, Henry. "Leaked APACHE Gunship video Iraq 2007: Two Reuters Reporters Killed Updated." *World News Vine.* 7 April 2010. http://worldnewsvine.com/2010/04/leaked-apache-gunship-video-iraq-2007-two-reuters-reporters-killed/. Accessed 25 April 2010.

"Israel Adds Cyber-Attack to IDF." *Defense Tech*. 11 February 2010. http://defensetech.org/2010/02/11/israel-adds-cyber-attack-to-idf/.

Jomini, Baron De. *The Art of War,* Translated by Capt. G.H. Mendell, and Lieut. W.P. Craighill. Radford, VA: Wilder Publications, 2008.

Kalb, Marvin and Dr. Carol Saivetz. "The Israeli-Hezbollah War of 2006: The Media as a Weapon in Asymmetrical Conflict." KSG Faculty Research Working Paper Series RWP07-012, February 2007.

Kelly, Kevin. *New Rules for the New Economy*. New York, N.Y.: Penguin Books Ltd., 1998.

Kenyon, Henry S. "US Army ponders Cyber Operations." *Signal*, October 2009.

Kuehl, Daniel T. "From Cyberspace to Cyberpower: Defining the Problem." In *Cyberpower and National Security*, edited by Franklin

D. Kramer, Stuart H. Starr, and Larry K. Wentz, 24-42. Washington, D.C.: National Defense University Press, 2009.

McCormack, Timothy L. *Self-Defense in International Law: The Israeli Raid on the Iraqi Nuclear Reactor*. New York, N.Y.: St. Martin's Press, 1996.

McCrystal, Stanley. Commander's Initial Assessment, 30 August 2009.

McCrystal, Stanley. "ISAF Commander's Counterinsurgency Guidance," 2009.

McFate, Montgomery. "Does Culture Matter? The Military Utility of Cultural Knowledge." *Joint Forces Quarterly 38*. Summer 2005, 43–46.

McLeary, Paul. "High-Tech Weapons Are Standard Issue for Insurgents," *Aviation Week*, 13 February 2008. http://www.aviationweek.com/aw/generic/story_generic.jsp?channel=dti&id=news/DTIINSURTECH.xml&headline=high-Tech%20Weapons%20Are%20Standard%20Issue%20For%20Insurgents. Accessed 26 April 2010.

MacAskill, Ewen. "New Cyber Security Chief Warns of Internet Attacks." (guardian.co.uk: Guardian News & Media Limited, 21 April 2010). http://www.concept-team.ch/2010/04/21/new-cyber-security-chief-warns-of-internet-attacks/. Accessed 25 April 2010.

Markoff, John and David Barboza. "Two China Schools Said to Be Tied to Online Attacks." *The New York Times*, 18 February 2010.

Matthews, Matt. "The Israeli defense Forces Response to the 2006 War with Hezbollah." *Military Review*, Vol. 89 Issue 4, Jul/Aug 2009.

Nakashima, Ellen. "Google to enlist NSA to help it ward off cyber attacks." *The Washington Post*, 4 February 2010.

National Security Presidential Directive 54. Cyber Security and Monitoring. Washington D.C.: Government Printing Office, 2008.

Rapoport, David. "Terrorism." In *Encyclopedia of Government and Politics*, vol. 2. Edited by Mary Hawkesworth and Maurice Kogan. London: Routledge, 1992.

Reed, Brian. “A Social network Approach to Understanding an Insurgency.” *Parameters*, Summer 2007, 27.

Robertson, David. *The Routledge Dictionary of Politics*. New York, N.Y.: Routledge, 2003.

Rumsfeld, Donald. Transcript. Remarks on “Twenty-first Century Transformation of US Armed Forces.” National Defense University, Fort McNair, Washington, D.C., Thursday, January 31, 2002.

Salahuddin, Sayed. “Gunmen Destroy Mobile Phone Tower in Afghan South.” Reuters, 2 March 2008, http://www.alertnet.org/thenews/newsdesk/ISL175699.htm.

Schwartau, Winn. *Information Warfare: Chaos on the Electronic Superhighway*, 2nd ed. New York, N.Y.: Thunder’s Mouth Press, 1996.

Scott, John. *Social Network Analysis: A Handbook*. 2nd Ed. Newberry Park, CA: Sage, 2000.

Secretary of the Air Force. *Air Force Doctrine Document 2*. 3 April 2007.

Secretary of the Air Force, *Air Force Doctrine Document 3-12.* (Pending approval for publication), April 2010.

Schelling, Thomas C. *Arms and Influence*. New Haven, CT: Yale University Press, 1966.

Shackelford, Scott. “Estonia Two-and-a-half Years Later: A Progress Report on Combating Cyber Attacks.” *Information Policy*, 15 February 2010. http://www.i-policy.org/2010/02/estonia-two-and-a-half-years-later-a-progress-report-on-combating-cyber-attacks.html.

Sheehan, Neil. *A Fiery Peace in a Cold War: Bernard Schriever and the Ultimate Weapon*. New York NY: Random House, 2009.

Tanous, Stephen M. Interview with author. 23 February 2010.

US Army FM 3-24. *Counterinsurgency Field Manual*. Chicago, IL: University of Chicago Press, 2007.

US Joint Chiefs of Staff, *Joint Publication System, Joint Publication 1-01*. Washington D.C.:US Joint Chiefs of Staff, 15 April 1988.

US Joint Chiefs of Staff, *Information Operations, Joint Publication 3-13*. Washington D.C.:US Joint Chiefs of Staff, February 13, 2006.

US Joint Chiefs of Staff, *Joint Doctrine for Space Operations, Joint Publication 3-14*. Washington D.C.:US Joint Chiefs of Staff, 9 January 2009.

Unified Command Plan (UCP), Washington D.C.:US Joint Chiefs of Staff, December 2008.

Unpublished paper. An Information Operations Officer, Task Force Iron. "Deception 2.0: Deceiving in the Netwar Age."

Waltz, Edward. *Information Warfare: Principles and Operations*. Boston, M.A.: Artech House, 1998.

Watts, Duncan. *Six Degrees: The Science of a Connected Age.* New York, N.Y.: W. W. Norton & Company, 2004.